UNIVERSIDAD CARLOS III DE MADRID

ESCUELA POLITÉCNICA

DEPARTAMENTO DE INFORMÁTICA

PROYECTO DE FIN DE CARRERA

Ingeniería Técnica en Informática de Gestión

AUDITORÍA SOBRE APLICACIÓN WEB PARA LA GESTIÓN DE DATOS CLÍNICOS EN RELACIÓN CON EL CUMPLIMIENTO DE LA LEGISLACIÓN ESPAÑOLA EN MATERIA DE PROTECCIÓN DE DATOS.

Autor: Ricardo Ramírez de Antón Molina
Tutor: Sergio Pastrana Portillo
Julio 2014

Título: AUDITORÍA SOBRE APLICACIÓN WEB PARA LA GESTIÓN DE DATOS CLÍNICOS EN RELACIÓN CON EL CUMPLIMIENTO DE LA LEGISLACIÓN ESPAÑOLA EN MATERIA DE PROTECCIÓN DE DATOS.

Autor: Ricardo Ramírez de Antón Molina

Tutor: Sergio Pastrana Portillo

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día __ de _____ de 20__ en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

AGRADECIMIENTOS.

Para comenzar agradecer a mi tutor Sergio por aguantarme tanto tiempo y por toda la ayuda proporcionada para poder finalizar el proyecto y con él completar el largo camino iniciado hace ya varios años en esta universidad.

A mi familia y amigos por apoyarme desde el principio y estar conmigo en los malos y en los buenos momentos pasados.

A todos vosotros por hacerme ver que con esfuerzo y empeño los sueños que se persiguen se pueden conseguir.

Gracias.

RESUMEN.

El presente documento recoge el diseño y desarrollo del Proyecto Fin de Carrera: “Auditoría sobre aplicación web para la gestión de datos clínicos en relación con el cumplimiento de la legislación española en materia de protección de datos”. En este proyecto se ha implementado una auditoría a una aplicación web para la gestión de datos de una clínica de reproducción asistida, para comprobar si esta cumple con la legislación vigente en España en materia de protección de datos.

La auditoría recoge aspectos de seguridad tanto físicos, relacionados con el espacio donde están albergados los equipos que alojan la aplicación web, como informáticos, relacionados con la propia aplicación web y el servidor virtual donde se encuentra implementada la aplicación. Concretamente, en este proyecto se presentan las siguientes contribuciones:

- Una especificación de requisitos que debe cumplir la aplicación, tanto a nivel físico como lógico para cumplir con la legislación vigente en España (concretamente, con la Ley Orgánica de Protección de Datos).

- Una batería de pruebas cuya intención es corroborar si cada uno de estos requisitos se cumplen.

- Una especificación de medidas y procedimientos de seguridad a aplicar en el proceso de implantación de la aplicación web, necesarias para satisfacer aquellos requisitos que no se cumplen en el estado actual en el que se encuentra el servidor.

ABSTRACT.

This document describes the design and development of the Final Degree Project entitled: "Audit of Web application for clinical data management regarding compliance with Spanish legislation on data protection." This project has developed an audit of a web application that manages data from a fertility clinic, in order to corroborate whether it satisfies current legislation in Spain in the field of data protection.

The audit considers both physical security, related to the room and space where the machines are allocated, and logical security, related to the web application itself and the server where it is hosted. Concretely, this projects presents the following contributions:

- A specification of physical and logical security requirements that the application must meet in order to comply with the Spanish law of data protection.

- A battery of tests and experiments to verify whether these requirements are met or not.

- A set of measures to be applied within the deployment of the web application in real settings, with the purpose of solve the problems encountered so as to comply with those requirements that are currently not met.

Contenido.

Índice de figuras.

Índice de tablas.

1. INTRODUCCIÓN.

En este proyecto se va a realizar una auditoría sobre una aplicación web relacionada con una clínica de reproducción asistida, en la que se manejan datos personales de los pacientes, para que cumpla con la normativa vigente en España.

A continuación, se comentará el contexto en el que se sitúa el proyecto, así como las principales motivaciones y objetivos planteados al inicio del desarrollo del mismo.

1.1. CONTEXTO.

Los datos personales (nombre, DNI, correo electrónico…) son habitualmente utilizados para identificar a las personas en el mundo virtual. Esta información la facilitamos a terceros en gran cantidad de escenarios: matriculación en un colegio o universidad, contrato de línea telefónica, transacciones bancarias, etc. Esto implica, gracias a la constante evolución de las TIC's, que se pueda realizar una utilización inadecuada de nuestros datos si estos no se encuentran convenientemente protegidos.

Es importante destacar la gran importancia que tiene la protección de los datos personales en nuestro Estado, siendo este un derecho fundamental de todos los españoles y recogido en la Constitución Española en sus artículos 10.1 (dignidad de las personas), 18.1 (derecho al honor y a la intimidad) y 18.4 (limitación de la informática por la ley):

Asimismo esta protección también viene recogida en una ley promulgada expresamente para este fin: la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). Ésta recoge en su artículo inicial:

> *La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.*

En esta ley y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, se basarán varios de los aspectos considerados en el desarrollo del presente proyecto.

Muchas de las empresas que realizan tratamiento de datos personales no cumplen con la legislación, lo que conlleva a severas penalizaciones económicas por parte de la Agencia Española de Protección de Datos (AGPD). (1). Por otro lado, únicamente 3 de cada 10 cumple en su totalidad con los requisitos de la LOPD.

DENUNCIAS Y RECLAMACIONES REGISTRADAS

TIPO	2010	2011	2012	VAR.% 2011/12
Escritos de reclamación de tutela	1.657	2.230	**2.193**	-1,66
Escritos de denuncia	5.045	7.648	**8.594**	12,37
TOTAL	**6.702**	**9.878**	**10.787**	**9,20**

DENUNCIAS Y RECLAMACIONES RESUELTAS

TIPO	2010	2011	2012	VAR.% 2011/12
Reclamaciones de tutela de derechos resueltas	1.830	1.939	**2.163**	11,55
Denuncias resueltas	5.122	5.917	**8.832**	49,26
TOTAL	**6.952**	**7.856**	**10.995**	**39,96**

Figura 1: Denuncias y reclamaciones de 2010 a 2012.

Este aumento en el número de denuncias y reclamaciones se debe a que los ciudadanos cada vez tienen más conocimiento sobre sus derechos, recogidos en la LOPD, lo que ha repercutido en un aumento del 7.43% en la recaudación de dinero por sanciones impuestas a las empresas llegando a alcanzar más de 21 millones de euros. Las personas que pueden ser sancionadas por las irregularidades cometidas en el cumplimiento de la ley son los responsables de los ficheros junto con los encargados del tratamiento de la información de carácter personal de las personas.

Las sanciones que se pueden llegar a imponer por el incumplimiento de la legislación se pueden clasificar en: leves (con multa de 900€ a 40.000€), graves (con multa de 40.001€ a 300.000€) y muy graves (con multa de 300.001€ a 600.000€).

1.2. MOTIVACION.

Este proyecto surge como consecuencia de la necesidad por parte de los sistemas de información de cumplir con esa reglamentación sobre protección de datos, con el fin de evitar sanciones. Concretamente, se propone la elaboración de una auditoría sobre una aplicación informática que contiene datos sensibles de carácter sanitario además de datos personales.

Con este proyecto se desea que la aplicación cumpla con todos los requisitos legales vigentes en la legislación española y así poder ser utilizada con total tranquilidad de no ser sancionados por la autoridad pertinente realizando una auditoría dirigida tanto a los aspectos informáticos (aplicación web, servidor donde se aloja…) como a los físicos (instalaciones donde están los sistemas informáticos).

Este proyecto es el tercero de un conjunto de proyectos que componen un proyecto global en el que se recogen las especificaciones para la creación de un sistema de gestión de datos sobre reproducción asistida en una clínica de fecundación in vitro. Dicho proyecto global se ha desarrollado en varios proyectos parciales:

1. El primer proyecto consistía en el diseño de la base de datos con la que se iba a tratar la información, que tipo de datos eran necesarios y cuáles eran los importantes que había que incluir, ya que en los ciclos de reproducción asistida se utiliza una gran cantidad de información, junto con el tratamiento que se deseaba dar a dicha información (2).
2. En el segundo, se implementó esa base de datos y se desarrolló una aplicación web para que los usuarios de la clínica de fecundación pudiesen hacer, de forma ágil y sencilla, un uso adecuado de los datos relacionados con sus pacientes (3).
3. El tercero de los proyectos, el cual se detalla en la presente memoria, está enfocado en la realización de una auditoría de seguridad de la aplicación desarrollada en el proyecto anterior para que cumpla con el ordenamiento jurídico vigente en España y pueda ser implantada en un entorno empresarial real.
4. En el cuarto proyecto, todavía por desarrollar, se implementará un sistema de toma de decisiones a partir de inteligencia artificial (data warehouse, minería de datos…) para facilitar la elección de los embriones más apropiados para realizar un tratamiento de reproducción asistida óptimo.

1.3. OBJETIVOS.

El objetivo principal es **realizar una auditoría informática a una aplicación web sobre reproducción asistida de una clínica que contiene datos personales de pacientes (datos de filiación, historial clínico…) que deben ser convenientemente protegidos, para que cumpla con la legislación española y pueda ser utilizada correctamente sin sufrir posibles sanciones.** La consecución de este objetivo generará como resultado una guía de operaciones y soluciones a implementar previas a la implantación de la aplicación en un entorno de producción.

Además de este objetivo principal se obtienen otros objetivos secundarios:

- Estudio de toda la reglamentación relacionada con la protección de datos personales, con el derecho al honor e intimidad de las personas (Constitución Española, Ley Orgánica de Protección de Datos, Código Penal…).
- Análisis exhaustivo de la aplicación web para determinar el correcto cumplimiento de la legislación estudiada, mediante la realización de una batería de pruebas completa.
- Test de penetración para evaluar las posibles vulnerabilidades del sistema informático y físico que contienen los datos sensibles de la aplicación.
- Definición de soluciones a todo error de diseño en la aplicación que contradiga las bases marcadas en la legislación para estar dentro del marco de la legalidad y poder ser utilizada sin problemas.
- Definición de soluciones a vulnerabilidades informáticas que pudiesen poner en peligro los datos de la clínica.

2. ESTADO DEL ARTE.

En este capítulo primero se revisará el estado actual en el que se encuentra el sistema sobre el que se ha realizado la auditoría. Luego, se definirán términos importantes para el entendimiento de este proyecto, así como la normativa aplicable y la reglamentación en la que nos apoyamos para hacer dicha auditoría. Finalmente se presentan las herramientas de análisis de vulnerabilidades utilizadas en el proyecto.

2.1. DESCRIPCION DEL SISTEMA.

Se ha mencionado con anterioridad que este proyecto está encuadrado en un grupo de proyectos, de los cuáles el segundo, *"Aplicación web para la gestión de datos clínicos relativos a los servicios de reproducción asistida humana"*, realizó el diseño e implementación de la aplicación web sobre la que se realizará la auditoría.

Dicha aplicación permite gestionar y tratar datos relativos a los pacientes de una clínica de reproducción asistida como son los datos personales de los pacientes, datos de informes clínicos o resultados de exploraciones médicas. Para el desarrollo de la aplicación web se ha utilizado eclipse, que es un entorno de desarrollo integrado que facilita el desarrollo de proyectos en JAVA. Como contenedor de servlets se utiliza Apache Tomcat, para recibir las peticiones de la aplicación web y redireccionarlas a un objeto servlet. La base de datos está implementada con MySQL, y para las consultas se utiliza la herramienta jQuery.

En cuanto a la aplicación web en sí, lo primero que hay que destacar son los diferentes perfiles de usuario que pueden acceder al sistema, estos están regidos por un sistema de roles y permisos que no permite que los usuarios puedan acceder a cualquiera de las opciones que propone el sistema, únicamente a aquellas a las que el administrador del sistema les dé permiso. Los diferentes perfiles son: paciente, embriólogo, laboratorio, ginecólogo, personal de administración, gestor de embriones y administrador web.

El sistema nos permite una serie de funcionalidades, las cuales pueden resumirse en **siete grandes bloques:**

- **Gestión del sistema:** Se enmarcan las operaciones no funcionales del sistema, login, registros de accesos y consultas. En este subsistema tenemos la opción de autenticarnos, mediante la introducción de un usuario y una contraseña proporcionada por el administrador del sistema podemos autenticarnos y así entrar en la aplicación web.

- **Gestión de pacientes:** En este bloque se tratan los datos personales de los pacientes. Dentro de este bloque podemos realizar tres opciones que son registrar pacientes, consultar datos personales y modificar esos datos personales.

  Con la primera opción, registro de pacientes, podemos introducir en la base de datos del sistema a los pacientes que acuden a la clínica para comenzar a realizar los tratamientos de reproducción asistida.

  La segunda, consulta de datos personales, se pueden observar cualquier dato personal de los introducidos cuando se han registrado los pacientes.

  Con la última de las opciones posibles en este grupo, modificación de datos personales, se pueden modificar cualquiera de los datos registrados en la base de datos en el caso de que estén introducidos de forma errónea.

- **Gestión de muestras:** Se encuentran en este grupo todos los datos relativos a las muestras obtenidas de los pacientes. Se pueden encontrar las opciones gestión de muestras de semen, gestión de biopsia y gestión de seminograma.

  Con gestión de muestra de semen, se puede introducir en el sistema los resultados obtenidos de muestras de semen de pacientes, verlos o modificarlos en caso de encontrar algún error.

  Gestión de biopsia permite introducir, consultar y modificar los datos relativos a las biopsias realizadas a los pacientes.

  En el último caso de este grupo está gestión de seminograma donde se pueden realizar las tareas de inserción, consulta y modificación de datos referentes a seminogramas de pacientes de la clínica.

- **Gestión de la historia clínicas:** Aquí se realiza el tratamiento de los datos personales que conforman el historial clínico de cada paciente. Este grupo lo forman las acciones gestión de anamnesis, gestión de serología, gestión ecografía, gestión exploración, gestión citología y gestión antecedentes.

  La gestión de anamnesis permite la introducción, modificación y consulta de todos los datos relativos a la anamnesis de cualquiera de los pacientes. Se pueden encontrar datos relativos a exploraciones, serologías, ecografías y citologías.

Mediante la gestión de serología se permite registrar, modificar y consultar los datos recogidos en una serología asociada a una anamnesis determinada.

Con la gestión de serología se pueden introducir, modificar y consultar la información incluida en las pruebas de serologías asociadas a un número de anamnesis.

La gestión de exploración deja registrar, modificar o consultar los datos relativos a exploraciones a los pacientes y que se encuentran relacionadas a una anamnesis determinada.

La gestión de citología permite introducir, consultar y modificar los datos obtenidos en citologías realizadas a pacientes de la clínica, estas citologías están asociadas a un número de anamnesis determinado.

La última de las opciones, gestión de antecedentes, permite introducir, modificar y consultar datos relacionados con los antecedentes clínicos de los pacientes de la clínica. Los antecedentes están relacionados a un número de anamnesis.

- **Gestión de tratamientos:** Se incluyen las diferentes pruebas que son realizadas a los pacientes.

  La primera de las acciones posibles, gestión de estimulación, permite dar de alta, modificar o consultar alguna de las estimulaciones asociadas a alguno de los pacientes en sus tratamientos de reproducción asistida.

  La siguiente opción es gestión de inseminación, la cual permite insertar en el sistema, modificar o consultar cualquiera de las inseminaciones realizadas a las pacientes registradas en el sistema.

  Por último, en gestión de ciclo de FIV se introducen, modifican y consultan los datos relativos a los ciclos de fecundación in vitro asociados a alguno de los pacientes.

- **Gestión de embriones:** Aparecerá toda la información relativa a los embriones guardados en el sistema.

  En alta de embriones podemos realizar el registro de los embriones del sistema asociados siempre a alguno de los pacientes de la clínica.

Modificación de embriones permite cambiar datos referentes a los embriones asociados a los pacientes a excepción del paciente y la muestra de semen asociados.

Con consulta de embriones podemos, mediante un número de identificación de cada embrión, observar los datos incluidos en cada registro de embrión.

- **Gestión de documentos:** Estarán encuadradas aquí todas las operaciones en las que los médicos envíen documentos a los pacientes, o sean estos últimos los que remitan esos documentos firmados electrónicamente.

  La primera de las opciones de este grupo es visualización de documentos, que nos permite consultar todos aquellos documentos médicos guardados en el sistema.

  Descarga de documentos nos permite guardar en nuestro equipo informático personal los documentos médicos con la finalidad de consultarlos o firmarlos en caso de que sea necesario para algún tipo de consentimiento.

  Envío de documentos a firmar, el personal médico de la clínica puede transferir a los pacientes documentación que es necesaria firmar para que estos den su consentimiento para la recolección de datos o realización de pruebas.

  Otra de la opciones que aparecen en este grupo es firma de documento, en la cual, un paciente puede firmar cualquier documento médico o de consentimiento gracias a esta opción sin necesidad de acudir a la clínica.

  La última de las opciones que se incluyen en este bloque es envío de documentos firmados, en la que los pacientes pueden remitir a los médicos de la clínica los documentos firmados.

Es sistema actualmente se encuentra alojado en una máquina virtual en un PC del departamento de informática de la Universidad Carlos III de Madrid, en una sala de trabajo del propio departamento. Al ser este un entorno de desarrollo, no se han aplicado medidas de seguridad física ni lógica específicas para el tratamiento de datos sensibles. Precisamente, en este proyecto se evalúa dicha seguridad y se proponen una serie de prácticas a aplicar para su implantación en entornos reales.

2.2. TERMINOS DE RELEVANCIA.

En este apartado se definirán ciertos términos necesarios para el correcto entendimiento del proyecto.

Dato sensible o especialmente protegido.

La definición que la RAE da al término dato es:

1. Antecedente necesario para llegar al conocimiento exacto de algo o para deducir las consecuencias legítimas de un hecho.

2. Información dispuesta de manera adecuada para su tratamiento por un ordenador.

Este tipo de dato viene regulado en el artículo 7 de la LOPD y se define como:

"Un tipo de datos que poseen gran relación con derechos y libertades públicas de las personas y por esta razón debe proporcionarse una mayor protección que al resto de datos personales". Se consideran datos sensibles los siguientes:

- Datos que revelen la ideología, afiliación sindical, religión y creencias.

- Datos que hagan referencia al origen racial, la salud o la vida sexual.

- Datos relativos a la comisión de infracciones penales o administrativas.

Auditoría.

Una auditoría es la evaluación realizada mediante la utilización de diferentes herramientas y técnicas de revisión, que tiene como objetivo la creación de un informe en el que se reflejen los diferentes errores, omisiones o irregularidades que afecten al sistema auditado con la finalidad de prevenirlos, detectarlos y/o corregirlos.

Auditar consiste en una doble comparación entre lo que se hace con lo que se debería hacer y lo que existe con lo que debería existir. Surgen diferentes definiciones entre las que se puede destacar:

-Norma AENOR X50-109:

Examen metódico de una situación relativa a un producto, proceso, organización, en materia de calidad, realizado en cooperación con los interesados, a fin de verificar la concordancia de la realidad con lo preestablecido, y la adecuación al objetivo buscado.

-Ley 19/1988 de Auditoría de Cuentas:

"... la actividad que, mediante la utilización de determinadas técnicas de revisión, tiene por objeto la emisión de un informe acerca de la fiabilidad de los documentos contables auditados; delimitándose, pues, a la mera comprobación de que los saldos que figuran en sus anotaciones contables concuerdan con los ofrecidos en el balance y en la cuenta de resultados,...".

Las auditorías pueden clasificarse desde distintos puntos de vista, estos son:

Según la persona que la realiza:

- Auditoría interna: realizada por empleados de la misma empresa, revisa cada departamento, centro o instalación con cierta periodicidad, sin eliminar el factor sorpresa.
- Auditoría externa: realizada por personal profesional ajena a la empresa e independientes, suelen realizar revisiones con una periodicidad mayor (anuales o bianuales).

Según su contenido y fines:

- Auditoría informática: examen y verificación de sistemas informáticos y su entorno.
- Auditoría de gestión: afecta a la situación global de la empresa, los temas que abarca son: dirección y gestión de los sistemas de información, gestión de recursos humanos, contratación de bienes y servicios, gestión de problemas y cambios, calidad y documentación.
- Auditoría de la organización y planificación: análisis de las diferentes áreas de la pirámide organizativa de la empresa.
- Auditoría de calidad: Para determinar si los procesos y los productos satisfacen las normas y estándares en cuanto a calidad para cubrir los objetivos generales.
- Auditoría de los datos: afecta a los diferentes tipos de datos tratados en la empresa.
- Auditoría de bases de datos: permite medir, demostrar y registrar los accesos a la información recogida en una base de datos.
- Auditoría de la seguridad: se centra en la comprobación de ciertos mecanismos que aseguran un buen funcionamiento de sistemas de seguridad como precaución a que estos fallen, se frustre o se violente.

- Auditoría de la seguridad física: afecta a la protección de hardware y soportes de datos junto con la seguridad de edificios e instalaciones que lo albergan ante situaciones de incendio, inundaciones, robo, sabotaje…
- Auditoría de la seguridad lógica: se centra en aspectos técnicos desde el diseño de la arquitectura hasta mecanismos de protección desarrollados para hacer frente a incidentes lógicos.

Según su amplitud:

- Auditoría total: afecta a todos los elementos de la empresa.
- Auditoría parcial: sólo afecta a diferentes partes de la empresa.

La realización de una auditoría se podría estructurar en tres fases:

-Trabajo preparatorio.

- Encargo: mediante propuesta, contrato del interesado.
- Planificación general.
- Programa de trabajo.

-Trabajo de campo.

- Revisiones, entrevistas, pruebas…
  - Pruebas de cumplimiento: Para determinar si el sistema de control interno funciona adecuadamente según la documentación, conforme aseguran los auditados, según las políticas y procedimientos de la entidad.
  - Pruebas sustantivas: Para obtener suficientes evidencias y que el auditor se forme un juicio mediante observación, cálculos, muestras para verificar la validez de la información.
  - Análisis y evaluación.

- Fase de informe.

Análisis de seguridad.

Conforma el estudio minucioso tanto de los recursos físicos como lógicos con la finalidad de identificar en ellos cualquier riesgo potencial al que pueda ser vulnerable un sistema y el desarrollo de soluciones que eliminen o controlen esos riesgos. Los pasos básicos para realizarlo son:

1. Seleccionar el sistema a analizar.
2. Identificar los riesgos de vulnerabilidades potenciales.

3. Desarrollar maneras de mitigar los riesgos que pueden poner en peligro el sistema.

Test de penetración.

Es un método para la evaluación de la seguridad existente en dispositivos y redes de comunicación simulando un ataque informático a un servidor o red de forma externa o interna. Radica en un análisis de todos los sistemas para la detección de vulnerabilidades de seguridad. Estos test son importantes para:

- Identificar vulnerabilidades de alto riesgo por combinación de otras de menor riesgo.
- Identificar vulnerabilidades imposibles de detectar por software de detección de vulnerabilidades.
- Probar la capacidad defensiva del sistema para detectar con éxito y dar una respuesta a los ataques.

El test de penetración está compuesto por dos fases:

- Test de penetración externo: cuyo objetivo es el acceso a los sistemas de forma remota y suplantar al administrador del sistema. Está compuesto por diferentes pruebas como pueden ser: captura de tráfico, scanning de puertos…
- Test de penetración interno: intenta demostrar cual es el nivel de seguridad interno. También está compuesto por diversas pruebas como autenticación de usuarios, verificación de permisos y recursos compartidos…

2.3. ESTANDARES Y NORMATIVA APLICABLE.

Agencia Española de Protección de Datos (AEPD). Creada en 1993, es la encargada en nuestro país de controlar el correcto cumplimiento de la reglamentación sobre la protección de datos de carácter personal. Tiene su sede en Madrid aunque su ámbito de actuación comprende todo el territorio nacional. Viene regulada en el título VI de la LO 15/1999 en la se dice que es "*un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones".* Algunas de las funciones de este ente son:

General:

- Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

En relación con los afectados:

- Atender a sus peticiones y reclamaciones.
- Información de los derechos reconocidos en la Ley.
- Promover campañas de difusión a través de los medios.

En relación con quienes tratan datos:

- Emitir autorizaciones previstas en la Ley.
- Requerir medidas de corrección.
- Ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos.
- Ejercer la potestad sancionadora.
- Autorizar las transferencias internacionales de datos.

En la elaboración de normas:

- Informar los Proyectos de normas de desarrollo de la LOPD y aquellos que incidan en materias de protección de datos.
- Dictar Instrucciones y recomendaciones de adecuación de los tratamientos a la LOPD.
- Dictar recomendaciones en materia de seguridad y control de acceso a los ficheros.

En materia de telecomunicaciones:

- Tutelar los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalente

Otras funciones:

- Velar por la publicidad en los tratamientos.
- Cooperación Internacional.
- Representación de España en los foros internacionales en la materia.
- Control y observancia de lo dispuesto en la Ley reguladora de la Función Estadística Pública.
- Elaboración de una Memoria Anual, presentada por conducto del Ministro de Justicia a las Cortes.

Figura 2: Agencia Española de Protección de Datos.

Actualmente el director de la AEPD es D. José Luis Rodríguez Álvarez, que ostenta la representación de la agencia y fue nombrado por Real Decreto a propuesta del Ministro de Justicia. La estructura de la agencia se puede ver en el siguiente esquema.

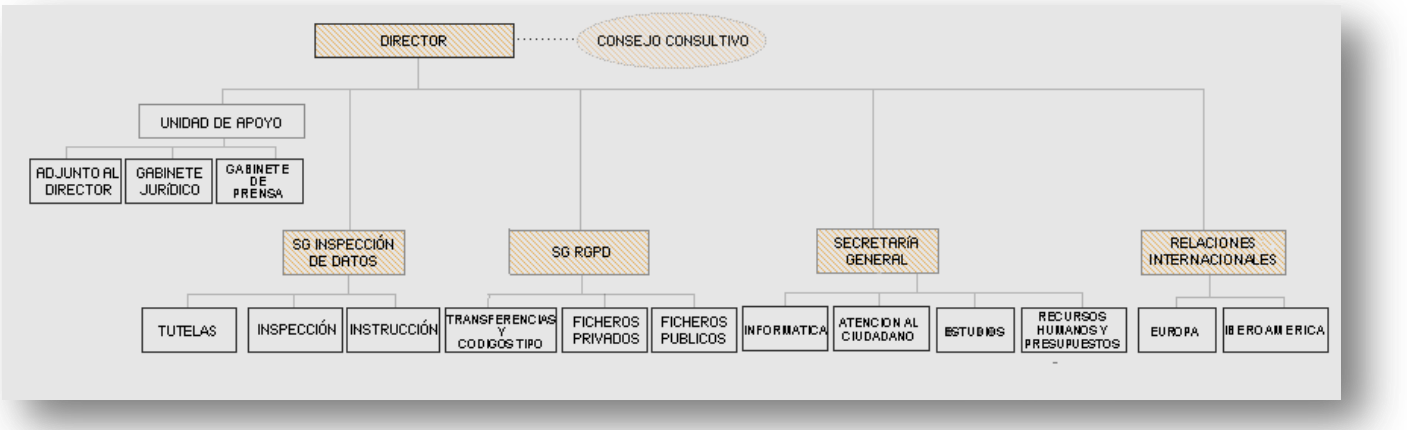

Figura 3: Organigrama de la APGD.

Ley Orgánica de 29 de Octubre de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. Realizada para desarrollar lo previsto en el artículo 18.4 de la Constitución Española, "*la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".*

El objetivo de esta ley es limitar el uso de medios informáticos y otras técnicas de tratamiento automatizado de datos personales para garantizar los derechos al honor e intimidad de los ciudadanos. Fue una de las medidas iniciales en nuestro país para la protección de datos personales, la ley ha sido derogada por la LOPD de la que se hablará más adelante.

Ley Orgánica 10/1995, de 23 de noviembre o Código Penal. Para dar más importancia a la protección de los datos el Estado incluyó un tipo penal, delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio en el Título X del Libro II, incluidos en el capítulo primero los relacionados con el descubrimiento y revelación de secretos, dedicando los artículos del 197 al 201 ambos inclusive.

> Artículo 197: Comprende el supuesto de hecho y las consecuencias jurídicas de este tipo penal.
>
> Artículo 198: Agravante del tipo penal por ser autoridad o funcionario público.
>
> Artículo 199: Supuesto de hecho y consecuencias jurídicas por ser realizado por personas que por razón de su oficio tengan conocimiento de secretos.
>
> Artículo 200: Ámbito de aplicación de este tipo penal.
>
> Artículo 201: Necesidad de denuncia para proceder por estos delitos anteriores.

Orientaciones para la constitución de zonas de acceso restringido. Es un documento realizado por la Oficina Nacional de Seguridad, órgano de trabajo del director del Centro Nacional de Inteligencia (CNI), para la construcción de zonas de acceso restringido. Se toma este documento como referencia para la evaluación de los sistemas de seguridad físicos ya que el órgano que lo ha creado es uno de los más importantes entes relacionados con la seguridad.

En él se tratan diferentes aspectos relacionados con la seguridad:

- Zonas de seguridad.
- Acreditación de una zona de acceso restringido.

- Medidas específicas de seguridad física (puertas, iluminación, control de acceso…).
- Equipamiento de seguridad.
- Seguridad física para los sistemas de información y comunicaciones.

Figura 4: Centro Nacional de Inteligencia.

2.4. LOPD, NIVEL DE DATOS.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Fue publicada en el Boletín Oficial del Estado (BOE) el 14 de diciembre de 1999 y entró en vigor el 14 de enero del siguiente año. Consta de siete títulos, cuarenta y nueve artículos, seis disposiciones adicionales, tres disposiciones transitorias, una disposición derogatoria y tres disposiciones finales. Con esta ley queda derogada la Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos (LORTAD) que estuvo en vigor durante siete años.

Esta ley tiene como objetivo garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar en lo concerniente al tratamiento de datos personales. Su estructuración es la siguiente:

- Título I: Disposiciones generales. Artículos 1 a 3.
- Título II: Principios de la protección de datos. Artículos 4 a 12.
- Título III: Derechos de las personas. Artículos 13 a 19.
- Título IV: Disposiciones sectoriales. Artículos 20 a 32.
    - Capítulo I: Ficheros de titularidad pública.
    - Capítulo II: Ficheros de titularidad privada.
- Título V: Movimiento internacional de datos. Artículos 33 a 34.
- Título VI: Agencia de Protección de Datos. Artículos 35 a 42.
- Título VII: Infracciones y sanciones. Artículos 43 a 49.

Cabe destacar que en apoyo a esta ley se aprobó el Real Decreto 1720/1999, de 13 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de protección de datos de carácter personal. El reglamento comparte con la Ley Orgánica la finalidad de combatir contra los riesgos que supone el tratamiento de datos personales. Esta norma reglamentaria nace con la inspiración de desarrollar los principios recogidos en la Ley y no de reiterar sus contenidos. El reglamento está formado por un total de 158 artículos encuadrados en 9 títulos.

2.5. HERRAMIENTAS DE ANALISIS.

Metasploit.

Es un software de pruebas de penetración que proporciona información acerca de posibles vulnerabilidades que pueda tener un sistema informático. Se utiliza como herramienta para ejecutar y desarrollar exploits contra un sistema remoto y así poder comprobar cuál es el estado de la seguridad de la máquina y si esta es efectiva o no.

Figura 5: Metasploit.

Metasploit incluye una serie de módulos como payloads (proporciona código que se puede ejecutar cuando un exploit ha sido exitoso), encoders (da algoritmos para codificar y ofuscar los playloads), exploits (se incluyen los diferentes exploits disponibles), post (proporciona funcionalidades para la fase post explotación), auxiliary (posibilita que actúen herramientas externas con el framework de Metasploit).

Nikto.

Es una herramienta de escaneo de servidores web con el que se pueden realizar diferentes acciones para la detección de vulnerabilidades o configuraciones erróneas en servidores web, detección de ficheros en instalaciones por defecto, listados con versiones y fechas de actualizaciones de servidores, ataques de fuerza bruta mediante diccionario… Una de las particularidades de esta herramienta es la posibilidad de crear reportes en diferentes formatos, junto con la posibilidad de integración con Metasploit.

Nessus.

Es un explorador de seguridad, con una amplia base de datos de plugins actualizada a diario, caracterizado por su facilidad de generar informes, exploración de hosts y búsqueda de vulnerabilidades en tiempo real.

Figura 6: Nessus.

Consiste en un proceso servidor que corre en segundo plano para facilitar el escaneo en la maquina objetivo y un programa cliente en el que se muestran los avances e informa de la progresión de los escaneos. Nessus comienza realizando un escaneo de puertos con nmap o su escaneador de puertos propio para después realizar diferentes exploits y atacarlos.

Nmap.

Se trata de una herramienta de código abierto para el análisis y escaneo de redes. Utiliza paquetes de IP sin ningún tipo de modificación para decretar que máquinas están disponibles en una red, los servicios que ofrecen junto con la versión de la aplicación, los sistemas operativos ejecutándose en ellos junto con sus versiones y los cortafuegos que están en uso.

Figura 7: Nmap.

El resultado que ofrece Nmap es un catálogo de objetivos analizados en el que proporciona información como puertos, protocolos utilizados, el nombre más común del servicio y su estado actual. También puede dar información acerca de los objetivos incluyendo nombres de DNS, sistema operativo disponible y direcciones MAC.

Evalúa.

Se trata de un programa creado por la AGPD que permite realizar, mediante la contestación de un simple test online, un análisis del grado en que se cumple la legislación vigente.

La aplicación crea, mediante las respuestas dadas por el propio usuario en el cuestionario, un informe en el que se orienta para cumplir la normativa mediante indicaciones y diferentes recursos.

Figura 8: Evalúa

Es un programa gratuito, anónimo, con un lenguaje claro fácil de comprender y que genera los informes con recomendaciones personalizadas, está disponible para todo aquel que quiera hacer uso de ella en la página web de la AGPD (4).

3. ANÁLISIS.

En este apartado se van a tratar los diferentes requisitos que debe cumplir nuestro sistema para cumplir con la reglamentación vigente. Se van a diferenciar dos bloques importantes, uno relacionado con la seguridad física del centro donde se van a encontrar los equipos que van a hacer que el sistema funcione con normalidad, y otro en el que se analizan los distintos componentes lógicos de la aplicación web.

3.1. REQUISITOS FISICOS.

Una parte importante en la seguridad es la correspondiente a los medios físicos de nuestro sistema: servidores, formularios con información sensible, etc… que deben ser debidamente protegidos para no poder ser manipulados por alguna persona no autorizada. A continuación se define el concepto seguridad física para posteriormente indicar en que ámbitos vamos a desarrollarla para poder proteger los componentes de nuestro sistema.

La seguridad física podría definirse como la aplicación de barreras físicas y controles preventivos, para minimizar y evitar amenazas y/o ataques contra los soportes físicos (hardware y medios de almacenamiento) que contienen información sensible. No hay que olvidar que estas amenazas se pueden dar tanto por personas (intento de entrada sin autorización, sabotajes,…) como por desastres naturales (incendios, inundaciones…) con lo que pueden darse diferentes supuestos.

Todos los equipos que integran nuestro sistema deben encontrarse en un CPD (Centro de Procesamiento de Datos) donde lo primero que vamos a controlar es el acceso al mismo para evitar riesgos como sabotajes o robos (ya sea de información o de los propios equipos).

Control de acceso al CPD.

- El CPD donde se almacenen los diferentes equipos encargados de guardar información y de hacer funcionar correctamente el sistema se encontrará en un área de acceso restringido protegido por una puerta con cerradura electromagnética. Para poder realizar la entrada se necesitará una tarjeta magnética y/o un código de seguridad que deberá ser proporcionado por el encargado de seguridad.

- Control de acceso automatizado, como se menciona anteriormente mediante el uso de tarjetas electromagnéticas, la entrega de estas tarjetas solo se realizara una vez hecho un registro anterior de la persona en el sistema donde se recogerán todos los datos personales por si hay algún tipo de incidencia.

- Asimismo se dispondrá de personal de seguridad que se encargará de la vigilancia del recinto en general y del personal que intentará acceder al CPD.

- Se dispondrá de un circuito cerrado de televisión, para complementar el trabajo del personal de seguridad. Además de poder dejar registrado en video cualquier incidencia, permite tener un mayor control en el caso de que surja cualquier tipo de catástrofe dentro del CPD como puede ser un incendio, etc… y actuar ante la situación con mayor brevedad.

- Disponer de contenedores de seguridad, cajas fuertes (ignífugas) para el alojamiento de servidores, copias de respaldo, documentos en formato papel.

Una vez mencionado las medidas de seguridad relativas al control de acceso al CPD abordaremos las relativas a otro tipo de amenazas de carácter natural: incendios, inundaciones y subidas de tensión.

Medidas contra incendios.

- Se dispondrá de una sala fabricada con materiales resistentes al fuego como el hormigón HCCA (Hormigón Armado Curado en Autoclave) protegida con una puerta ignífuga que posea un sistema de cerradura electromagnética.

- Se instalarán sistemas automáticos de extinción de incendios, en el caso del CPD serán sistemas de extinción por gases para no dañar los equipos en caso de activación del sistema de extinción.

- Se habilitará también dentro de la sala equipos de extinción de incendios portátiles, a poder ser de CO2 o alguna sustancia no peligrosa para los equipos. Es importante dar aviso de esto a los bomberos en caso de que tengan que realizar una intervención dentro del CPD.

- Armarios ignífugos para guardar cintas de backup y otros documentos y archivos con información importante.

- Situar un sistema de aire acondicionado que regule y controle la temperatura de la sala, la temperatura óptima para el funcionamiento y mantenimiento de los equipos seria entre 21 y 23 grados. El

sistema de control de temperatura estará conectado con la sala de seguridad para controlar con mayor eficacia los aumentos de temperatura producidos por un posible incendio.

Medidas contra inundaciones.

- Los techos y suelos del interior del CPD se fabricarán con materiales impermeables, además estará libre de cualquier tipo de canalización o desagüe que pueda romperse y causar cualquier tipo de problema.

- Las puertas del CPD se acondicionarán para ser capaces de contener el agua en el exterior del emplazamiento.

- Es necesario disponer de algún tipo de sistema capaz de interrumpir la electricidad en el caso de que se detecte que ha entrado agua y puede afectar a los equipos, para evitar que se produzcan cortocircuitos y evitar así un posible incendio posterior.

Medidas para la energía.

- El cableado de la sala (cables de alimentación de equipos, cables de red, de interconexión de equipos…) irá situado en un falso suelo para estar así más protegidos y evitar roturas accidentales, desconexiones.

- Se dispondrá de un sistema de alimentación ininterrumpida (SAI) para que, en caso de apagón o caída de la tensión los equipos puedan seguir funcionando con normalidad hasta que se restablezca el servicio normal.

- Disponer de servidores auxiliares en otra localización distinta al CPD para que si los equipos sufren problemas o alguna de las calamidades anteriormente citadas, no perdamos el servicio del sistema por completo.

3.2. ESPECIFICACIÓN DE REQUISITOS LÓGICOS.

En este apartado se va explicar la estructura con la que se van a mostrar los diferentes requisitos lógicos en forma de tabla de la manera siguiente.

Requisito	**(Id)**	**(Título)**	
Descripción	(Descripción)		
Origen	(Origen)		
Prioridad	( ) Requerido	( ) Deseable	( ) Opcional
Cambios		(Versión)	

Tabla 1: Tabla genérica especificación de requisitos.

- (Id): es el identificador inequívoco de cada requisito, sigue la siguiente denominación, RY_X. Donde Y puede tomar los valores S Sistema, A Aplicación o G Administrativo siendo X números secuenciales de identificación.
- (Título): Nombre del requisito.
- (Descripción): Explicación del requisito.
- (Origen): Quién o qué origina este requisito.
- Prioridad: Grado de necesidad de cumplir este requisito, pueden seleccionarse tres opciones diferentes. Requerido, es obligatorio cumplir el requisito, Deseable, no resulta obligatorio cumplir dicho requisito pero sería beneficioso si se hace, y por último opcional, se puede realizar siempre que se desee sin ninguna obligatoriedad.
- (Versión): Indica el número de versión en la cual nos encontramos.

3.3. REQUISITOS TÉCNICOS: SISTEMA.

En este primer conjunto de requisitos se recogerán todos aquellos relacionados con el sistema que aloja la aplicación web, y que serán de obligado cumplimiento de acorde con la legalidad vigente. En este conjunto están encuadrados requisitos como la asignación de un sistema de roles y permisos a los diferentes usuarios que luego accederán a la aplicación, registros de entradas al programa o la eliminación de datos en la base de datos que ya no sean necesarios mantener.

Requisito	RS_1	Identificación y autenticación.	
Descripción	Deberá haber un procedimiento de asignación y distribución de contraseñas para la identificación inequívoca de toda persona que acceda al sistema. Esas contraseñas serán guardadas de forma ininteligible.		
Origen	Legal. Artículo 93 del Reglamento de desarrollo de la LOPD.		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 2: RS_1 Identificación y autenticación.

Requisito	RS_2	Usuarios y autorizaciones.	
Descripción	Se deberá poder ver una relación actualizada de usuarios y accesos autorizados. Solo personal administrador.		
Origen	Legal. Artículo 91 del Reglamento de desarrollo de la LOPD.		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 3:RS_2 Usuarios y autorizaciones.

Requisito	RS_3	Control de accesos.	
Descripción	Control de accesos permitidos a cada usuario según las funciones asignadas (permisos que tenga el usuario).		
Origen	Legal. Artículo 91 del Reglamento de desarrollo de la LOPD.		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 4: RS_3 Control de accesos.

Requisito	RS_4	Permisos de acceso.	
Descripción	En la aplicación se podrá conceder, alterar o anular el acceso autorizado sobre los recursos. Esto solo lo hará el personal autorizado.		
Origen	Legal. Artículo 91 del Reglamento de desarrollo de la LOPD.		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 5:RS_4 Permisos de accesos.

Requisito	RS_5	Registro de accesos.	
Descripción	El sistema deberá guardar un archivo donde aparezcan todos los accesos, deberá aparecer: usuario, fecha y hora, fichero, tipo de acceso, si es un acceso autorizado o denegado.		
Origen	Legal. Artículo 103 del Reglamento de desarrollo de la LOPD.		
Prioridad	( ) Requerido	( ) Deseable	(*) Opcional
Cambios		Versión inicial	

Tabla 6:RS_5: Registro de accesos.

Requisito	RS_6	Accesos no autorizados.	
Descripción	La aplicación deberá disponer de los mecanismos necesarios para evitar accesos no autorizados.		
Origen	Legal. Artículo 9 de la LOPD.		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 7: RS_6 Accesos no autorizados.

Requisito	**RS_7**	**Eliminación de datos no viables.**	
Descripción	Al darse de baja un usuario, el sistema garantizará que todos sus datos de carácter personal serán convenientemente destruidos de forma que no se puedan recuperar.		
Origen	Legal. Artículo 4 de la LOPD.		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 8: RS_7 Eliminación de datos no viables.

Requisito	**RS_8**	**Límite de accesos.**	
Descripción	Se establecerá un mecanismo que limite los intentos de accesos no autorizados al sistema.		
Origen	Legal. Artículo 98 del Reglamento de desarrollo de la LOPD.		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 9: RS_8 Límite de accesos.

3.4. REQUISITOS TÉCNICOS: APLICACIÓN.

En este segundo grupo de requisitos se encuadrarán todos aquellos requerimientos que tengan relación directa con la aplicación web. Aquí se contemplan por ejemplo mecanismos para firmar consentimientos de clientes de la clínica, comprobación de firmas de documentos, un canal para realizar incidencias o métodos de copias de seguridad en caso de pérdida de datos.

Requisito	**RA_1**	**Consentimiento de los afectados.**	
Descripción	El sistema deberá añadir en los formularios de alta un consentimiento con el que deberá estar de acuerdo el paciente. Además de informar en ellos sobre el tipo de tratamiento se le va a realizar a esa información, quien va a ser la persona o personas que la van a tratar y a quien se le va a traspasar esa información añadiendo también ante que ente puede ejercer sus derechos ARCO (acceso, rectificación, cancelación y oposición).		
Origen	Legal. Artículo 6 de la LOPD		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 10: RA_1 Consentimiento de los afectados.

Requisito	**RA_2**	**Comunicación de cesiones de datos.**	
Descripción	Se comunicará a los clientes de la clínica cualquier tipo de cesión de sus datos personales. Antes de realizar la cesión hay que conseguir el consentimiento de los afectados.		
Origen	Legal. Artículos 11 y 27 de la LOPD.		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 11:RA_2 Comunicación de cesiones de datos.

Requisito	RA_3	Verificación de firma digital.	
Descripción	Se comprobará que la firma realizada por los clientes para dar su consentimiento es verdadera.		
Origen	Seguridad.		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 12:RA_3 Verificación de firma digital.

Requisito	RA_4	Comprobación emisor de certificado.	
Descripción	Verificaremos que la firma de los consentimientos ha sido realizada por los clientes y no por otras personas que pudieran suplantar la identidad de los clientes.		
Origen	Seguridad.		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 13:RA_4 Comprobación emisor de certificado.

Requisito	RA_5	Límite de accesos.	
Descripción	Se establecerá un mecanismo que limite los intentos de accesos no autorizados a la aplicación.		
Origen	Legal. Artículo 98 del Reglamento de desarrollo de la LOPD.		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 14:RA_5 Límite de accesos.

Requisito	RA_6	Cambio contraseñas.	
Descripción	El sistema avisará al usuario del deber de cambiar la contraseña si este no lo ha realizado en un periodo de 1 año como máximo.		
Origen	Legal. Artículo 93 del Reglamento de desarrollo de la LOPD.		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 15:RA_6 Cambio contraseñas.

Requisito	RA_7	Canal telemático para derechos ARCO.	
Descripción	Se deberá implementar un método por el cual los pacientes puedan acceder a sus datos personales para verlos, rectificarlos en el caso de que encuentren algún error en ellos, cancelarlos/darlos de baja si ya no son necesarios u oponerse a que sigan utilizándose sus datos.		
Origen	Legal. Artículos 15 y 16 de la LOPD.		
Prioridad	( ) Requerido	(*) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 16:RA_7 Canal telemático para derechos ARCO.

Requisito	RA_8	Registro de incidencias.	
Descripción	Deberá existir un servicio de notificación y registro de incidencias en el que aparecerá: tipo de incidencia, momento de su detección, persona que la notifica, a quien se comunica, efectos producidos por dicha incidencia y medidas correctoras aplicadas.		
Origen	Legal. Artículo 90 del Reglamento de desarrollo de la LOPD.		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 17:RA_8 Registro de incidencias.

Requisito	RA_9	Gestión de documentos y soportes.	
Descripción	Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado. En el caso de entrada/salida de soportes se deberá crear un registro en el que se incluya: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizado para recepción/entrega.		
Origen	Legal. Artículos 92 y 97 del Reglamento de desarrollo de la LOPD.		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 18:RA_9 Gestión de documentos y soportes.

Requisito	RA_10	Copias de respaldo.	
Descripción	El sistema deberá contar con un procedimiento para la realización de una copia de respaldo semanal, así como de procedimientos de generación de copias de respaldo y recuperación de datos en caso de pérdida o destrucción. Se deberá realizar una verificación semestral de los procedimientos de copias y recuperación. Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan.		
Origen	Legal. Artículos 94 y 102 del Reglamento de desarrollo de la LOPD.		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 19:RA_10 Copias de respaldo.

3.5. REQUISITOS ADMINISTRATIVOS.

En este último grupo de requisitos se encuentran todos aquellos que no tienen aplicación directa con el sistema, sino que tienen un carácter administrativo y procedimental. Por ejemplo, la obligación de notificar a la AGPD del uso de ficheros con datos personales, deber de guardar secreto los empleados de la clínica sobre los datos que puedan observar o la obligatoriedad de crear un documento de seguridad.

Requisito	**RG_1**	**Notificación a la Agencia de Protección de Datos.**	
Descripción	Hay que notificar a la Agencia de Protección de Datos de la creación de ficheros de datos de carácter personal.		
Origen	Legal. Artículo 26 de la LOPD		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 20:RG_1 Notificación a la AGPD.

Requisito	**RG_2**	**Deber de secreto.**	
Descripción	Se incluirá en el contrato del personal que tenga acceso a los datos de la aplicación una cláusula de confidencialidad.		
Origen	Legal. Artículo 10 de la LOPD		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 21:RG_2 Deber de secreto.

Requisito	**RG_3**	**Documento de seguridad.**	
Descripción	Se creará un documento de seguridad que recogerá las medidas de índole técnica y organizativa.		
Origen	Legal. Artículo 88 del Reglamento de desarrollo de la LOPD.		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 22:RG_3 Documento de seguridad.

Requisito	**RG_4**	**Medidas de seguridad nivel alto.**	
Descripción	Deberán implantarse las medidas de seguridad de nivel alto debido a que tratamos datos referentes a la salud o vida sexual. Estas medidas se recogen en el documento de seguridad.		
Origen	Legal. Artículo 7 de la LOPD.		
Prioridad	(*) Requerido	( ) Deseable	( ) Opcional
Cambios		Versión inicial	

Tabla 23:RG_4 Medidas de seguridad nivel alto.

4. PRUEBAS DE VERIFICACION DE REQUISITOS.

En este capítulo se definen todas aquellas pruebas realizadas con el fin de evaluar si los requisitos recogidos en el capítulo anterior se cumplen correctamente o no.

Esta batería de pruebas se ha dividido en dos partes, la primera en la que encuadraremos las pruebas realizadas directamente sobre el sistema, lo que en esta memoria se denomina testeo de la aplicación y una segunda correspondiente a todas aquellas relacionadas con la seguridad física.

La representación de estas pruebas se realizará mediante tablas que seguirán el siguiente formato:

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
(Id)	(Nombre)	(Descripción)	(Resultado)	(Requisito asociado)

Tabla 24: Tabla genérica de prueba de requisitos.

- (Id): Representa el identificador inequívoco de cada una de las pruebas realizadas, muestra la siguiente nomenclatura, PVR-XX, donde XX representa la secuencia de números para su identificación.
- (Nombre): Nombre que se le proporciona a la prueba.
- (Descripción): Muestra el camino que se ha seguido para la realización de cada una de las pruebas.
- (Resultado): Resultado obtenido en la prueba, representado con dos símbolos: ✓ para identificar un resultado positivo que implica el cumplimiento del requisito asociado y ✗ para identificar que el requisito no se cumple.
- (Requisito asociado): Identificador de los requisitos que se pretenden corroborar con cada una de las pruebas.

4.1. TESTEO APLICACIÓN.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-1	Consentimiento de afectados.	1. Un usuario con permisos para dar de alta nuevos usuarios, se autentica en la aplicación. 2. Selecciona la opción “Alta Nuevo Paciente”, introduce los datos del nuevo paciente y pulsa “Aceptar”. 3. El sistema debe crear un documento de consentimiento que tendrá que firmar el nuevo paciente.	✘ La aplicación no crea ningún documento de consentimiento .	RA_1

Tabla 25: PVR-1 Consentimiento de los afectados.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-2	Consentimiento de cesiones.	1. Un usuario ginecólogo se autentica en la aplicación. 2. Selecciona la opción “Ver documentos enviados”, luego pulsa el botón enviar documento. 3. Selecciona el paciente, el nombre del documento y el documento de consentimiento, por último selecciona enviar. 4. El usuario paciente hace login en la aplicación, selecciona “ver documentos a firmar”. Selecciona el documento a firmar, el tipo de certificado y da a enviar. 5. Enviado el documento el ginecólogo puede ver el documento firmado repitiendo los pasos 1 y 2.	✓ El documento se recibe debidamente firmado.	RA_2

Tabla 26: PVR-2 Consentimiento de cesiones.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-3	Acceso autorizado de usuario.	1. Intento de acceso al sistema con cualquiera de los usuarios guardados en el sistema (administrador, laboratorio, ginecólogo, embriólogo, secretaria o paciente) con nombre de usuario y contraseña correctos.	✓ Se accede al sistema correctamente.	RS_1

Tabla 27: PVR-3 Acceso autorizado de usuarios.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-4	Acceso no autorizado.	1. Intentar acceder al sistema con cualquiera de los usuarios guardados en el sistema (administrador, laboratorio, ginecólogo, embriólogo, secretaria o paciente) con su nombre de usuario y/o una contraseña incorrecta.	✓ No se accede al sistema. Da un aviso de usuario o contraseña incorrecta.	RS_1

Tabla 28: PVR-4 Acceso no autorizado.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-5	Acceso al servidor web.	1. Acceso al servidor con el usuario y contraseña de administrador.	✓ Se accede correctamente al servidor web.	RS_1

Tabla 29: PVR-5 Acceso al servidor web.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-6	Acceso no autorizado servidor web.	1. Acceso al servidor con cualquiera de los usuarios creados para entrar en la aplicación.	✓ El servidor no permite el acceso.	RS_1

Tabla 30: PVR-6 Acceso no autorizado al servidor web.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-7	Control usuarios y autorizaciones.	1. Acceso al servidor de la base de datos con usuario y contraseña de administrador. 2. Seleccionar mediante comandos SQL la tabla donde se guardan los datos referidos a los usuarios que tienen acceso al sistema.	✓ Al acceder a las tablas de usuarios se puede observar cada uno con su respectivo rol. ✘ Se puede ver las contraseñas de cada usuario en claro.	RS_2

Tabla 31: PVR-7 Control usuarios y autorizaciones.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-8	Registro de accesos.	1. Acceso al servidor de la base de datos con el usuario y claves del administrador. 2. Seleccionar de la base de datos la tabla accesos.	✓ Se muestra un listado con todos los usuarios qué han accedido al sistema y cuándo.	RS_5

Tabla 32: PVR-8 Registro de accesos.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-9	Registro zonas accedidas del sistema.	1. Acceder al servidor de la base de datos con el usuario y claves del administrador. 2. Seleccionar en la base de datos la tabla accesos.	✘ Se observa un listado con todos los usuarios que han accedido al sistema y cuando, pero no aparece a que partes del sistema acceden.	RS_5

Tabla 33: PVR-9 Registro zonas accedidas del sistema.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-10	Modificación de roles.	1. Acceso al servidor de la base de datos con el usuario y claves del administrador. 2. Acceder en la base de datos a la tabla de usuarios del sistema. 3. Cambiar el rol de alguno de los usuarios.	✓ Permite el cambio de roles, pero sólo en el caso de actuar como administrador.	RS_4

Tabla 34: PVR-10 Modificación de roles.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-11	Límite de accesos en el servidor de la base de datos.	1. Introducir en el servidor de la base de datos varias veces el usuario y la contraseña de forma incorrecta.	✓ El servidor bloquea el acceso y no deja volver a realizar más intentos. Hay que volver a conectar con el servidor para intentarlo de nuevo.	RS_8

Tabla 35: PVR-11 Límite de accesos en el servidor de la base de datos.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-12	Límite de accesos a la aplicación web.	1. Introducir en la aplicación web varias veces el usuario y la contraseña de forma incorrecta.	✘ Se permite la introducción de nombres de usuario y contraseñas erróneos de forma indefinida, sin sufrir ningún tipo de bloqueo.	RA_5

Tabla 36: PVR-12 Límite de accesos a la aplicación web.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-13	Acceso sin permisos.	1. Entrar al sistema como secretario (con permiso para dar de alta nuevo paciente y consultar/modificar datos de pacientes) intentar ver los antecedentes o las pruebas a un paciente distinto, sin permiso para ello. 2. Entrar al sistema como paciente (con permiso para consultar/modificar datos personales propios y recibir/enviar documentos médicos firmados) intentar ver los antecedentes o las pruebas a un paciente distinto, sin permiso para ello. 3. Entrar al sistema como personal de laboratorio (con permiso para buscar muestras) intentar ver los antecedentes o las pruebas a un paciente, sin permiso para ello.	✓ El sistema no da la opción de ver ni realizar acciones para lo que no se disponga del permiso correspondiente.	RS_3

Tabla 37: PVR-13 Acceso sin permisos.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-14	Cambio de contraseña.	1. Crear un nuevo usuario en el sistema. 2. Pasado un mes volver a entrar al sistema con ese usuario creado. 3. El sistema debe mandar un mensaje al usuario para cambiar la contraseña por seguridad.	✘ El sistema no da aviso alguno para cambiar la contraseña pasado un periodo de tiempo.	RA_6

Tabla 38: PVR-14 Cambio de contraseña.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-15	Ver ficha personal.	1. Acceder a la aplicación mediante usuario y contraseña de paciente. 2. Seleccionar la opción datos del paciente para consultar los datos personales.	✓ Se muestran los datos con los que se dio de alta el paciente en el sistema y no deja ver ningún otro paciente distinto.	RA_7

Tabla 39: PVR-15 Ver ficha personal.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-16	Modificar ficha personal.	1. Acceder a la aplicación mediante usuario y contraseña de paciente. 2. Entrar en datos del paciente. 3. Pinchar en editar datos personales.	✓ Permite modificar únicamente la dirección, ciudad, código postal, provincia y número de contacto.	RA_7

Tabla 40: PVR-16 Modificar ficha personal.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-17	Eliminar ficha personal.	1. Acceder a la aplicación mediante usuario y contraseña de paciente. 2. Entrar en datos del paciente.	✘ No hay posibilidad alguna para eliminar los datos guardados en el sistema desde la aplicación, la forma para hacerlo sería ponerse en contacto con el administrador del sistema para la eliminación de los datos mediante correo electrónico y sin entrar en la aplicación.	RA_7

Tabla 41: PVR-17 Eliminar ficha personal.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-18	Contacto derechos ARCO.	1. Acceder a la aplicación mediante usuario y contraseña de paciente para poner una incidencia.	✘ No hay opción ni botón alguno para poder realizar la incidencia ni formulario de contacto.	RA_7

Tabla 42: PVR-18 Contacto derechos ARCO.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-19	Eliminación de datos no viables.	1. Entrar a la aplicación como ginecólogo o secretario (personal cualificado para dar de baja algún paciente). 2. Buscar un paciente. 3. Intentar borrarlo del sistema.	✘ No hay opción en la aplicación de eliminar un paciente del que ya no son necesarios sus datos. Sólo es posible desde el servidor y por el administrador.	RS_7

Tabla 43: PVR-19 Eliminación de datos no viables.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-20	Realizar incidencia del sistema.	1. Entrar a la página web donde se encuentra la aplicación. 2. Seleccionar el enlace “¿necesitas ayuda?”.	✓ Sólo dispone de ese canal para realizar cualquier incidencia, desde perdida de contraseña a deseo de eliminación de la ficha personal de un paciente, dentro de la aplicación no hay posibilidad.	RA_8

Tabla 44: PVR-20 Realizar incidencia del sistema.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-21	Registro de incidencias.	1. Entrar al correo electrónico del administrador del sistema.	✓ Se puede ver un registro de incidencias siempre que el administrados no elimine los mensajes de las incidencias puestas por los clientes.	RA_8

Tabla 45: PVR-21 Registro de incidencias.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-22	Control documentación y soportes.	1. Entrar a la aplicación o al servidor web como administrador. 2. Buscar el archivo donde se encuentran recogidos los distintos soportes que forman el sistema.	✘ No aparecen en ninguno de los dos sitios una tabla donde se puedan recoger los documentos que se pudieran crear y los soportes que forman el sistema. Sólo se mantiene un listado de documentación que se intercambia entre médicos y pacientes.	RA_9

Tabla 46: PVR-22 Control documentación y soportes.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-23	Control sobre las pruebas médicas.	1. Acceder a la aplicación como ginecólogo. 2. Seleccionar “ver documentos enviados”.	✔ Aparece sólo la documentación que envía el médico que accede al sistema, la única forma de ver el resto de documentación es accediendo a la aplicación como los diferentes médicos que tengamos dados de alta en el sistema.	RA_9

Tabla 47: PVR-23 Control sobre las pruebas médicas.

ID	NOMBRE	DESCRIPCIÓN	RESULTADO	REQUISITO ASOCIADO
PVR-24	Accesos no autorizados.	1. Se realizan ataques al sistema con diversas herramientas.	✔ Se encuentran diferentes vulnerabilidades que se detallarán más adelante.	RS_6

Tabla 48: PVR-24 Accesos no autorizados.

El Sistema no proporciona ningún método para realizar copias de seguridad, con lo que no se cumplen el requisito RA_10.

A continuación aparece una tabla donde se recoge cada una de las pruebas realizadas y los requisitos que cumple cada una de ellas.

	RS_1	RS_2	RS_3	RS_4	RS_5	RS_6	RS_7	RS_8	RA_1	RA_2	RA_5	RA_6	RA_7	RA_8	RA_9
PVR-1									×						
PVR-2										✓					
PVR-3	✓														
PVR-4	✓														
PVR-5	✓														
PVR-6	✓														
PVR-7		×													
PVR-8					✓										
PVR-9					×										
PVR-10				✓											
PVR-11								✓							
PVR-12											×				
PVR-13			✓												
PVR-14												×			
PVR-15													✓		
PVR-16													✓		
PVR-17													×		
PVR-18													×		
PVR-19							×								
PVR-20														✓	
PVR-21														✓	
PVR-22															×
PVR-23															×
PVR-24						×									

Tabla 49: Tabla resumen de pruebas de verificación de requisitos.

*Los requisitos RA_3, RA_4, RA_10, RG_1, RG_2, RG_3 y RG_4 no aparecen en la tabla al no tener asignada prueba de verificación.

Como se puede observar en la tabla hay diferentes requisitos que no se cumplen en el sistema, lo que puede conllevar a fuertes sanciones económicas por parte de la administración, recogidas en la LOPD. Concretamente, algunas irregularidades y diferentes sanciones a las que se pueden enfrentar los responsables del sistema son las siguientes:

- Por los requisitos incumplidos RS_2, RS_5, RS_6, RA_5, RA_6 y RA_9 todos encuadrados en la falta de suficientes medidas de seguridad además de no seguir los principios y garantías de la LOPD, podría

enfrentarse a una sanción, siempre que se engloben todas como una única infracción, de 40.001 a 300.000€ al considerarse infracción grave. Si fueran por separado se estaría hablando de 240.006 a 1.800.000 €.

- Por el RS_7, de eliminación de datos no viables, se incurriría en una infracción grave con sanciones de 40.001 a 300.000€.
- Al no cumplir el RA_1, relacionado con el consentimiento de los pacientes, se puede ser sancionado por incidir en una infracción muy grave con sanciones de 300.001 a 600.000€.
- El RA_7 ligado a los derechos ARCO, supone una infracción leve con sanción de 900 a 40.000€.

Además de las sanciones mencionadas, el no cumplimiento de otros requisitos para los cuáles no se ha realizado pruebas de verificación puede conllevar a otras sanciones. Se van a señalar a continuación algunas de estas sanciones:

- RA_3 y RA_4 podrían englobarse en una única infracción grave referente a la seguridad suficiente del sistema sancionada con 40.001 a 300.000€.
- Los requisitos asociados que no siguen los principios y garantías de la LOPD: RG_3, RG_4 y RA_10 son sancionados con 40.001 a 300.000€ por ser consideradas graves.
- El requisito RG_1, de notificación a la AGPD es considerado como una infracción grave sancionada con 40.001 a 300.000€.
- Y por último hay que señalar el RG_2, relacionado con el deber de secreto que supone una infracción muy grave con sanciones de 300.001 a 600.000€.

En el peor de los casos, el **total** de todas estas infracciones podría conllevar a **sanciones** que irían de **800.907 a 2.740.000€.** Además, como se ha comentado anteriormente, si las sanciones se aplican individualmente a cada una de las infracciones, el montante total podría ascender hasta una **cifra máxima de 5.140.000€ en sanciones**.

4.2. TEST DE PENETRACIÓN.

A continuación se va a detallar más profundamente la prueba número 24, correspondiente al análisis de posibles accesos no autorizados. En esta prueba se utilizaron diferentes herramientas para detectar posibles vulnerabilidades en el sistema que pudieran poner en peligro los datos almacenados.

La primera acción que se realizó sobre el sistema fue un escaneo con la herramienta *nmap* utilizando su opción de escaneo intenso, a la dirección ip del sistema para poder determinar si alguno de sus puertos se encontraba abierto e intentar sacar algún tipo de información relevante sobre ellos.

En dicho escaneo básico de puertos sobre el servidor, esta es la información obtenida:

Port	Protocol	State	Service	Versión
22	tcp	open	ssh	OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)
80	tcp	open	http	Apache httpd 2.2.22 ((Ubuntu))
443	tcp	open	http	Apache httpd 2.2.22

Tabla 50: Escaneo de puertos del sistema.

Como se puede observar en la tabla superior se encontraron tres puertos diferentes del servidor, 22, 80 y 443 abiertos y las versiones de los sistemas operativos que están corriendo actualmente en cada uno de ellos.

Esto en realidad no es un problema muy grave ya que con esa información no se va a acceder directamente al sistema sin permiso, pero con la información obtenida acerca de protocolos, servicios y versiones obtenidos se pueden buscar vulnerabilidades que hayan sido detectadas en esas versiones específicas para intentar acceder al sistema sin autorización.

En sucesivos escaneos más profundos con la misma herramienta se pudo obtener mayor información acerca de los puertos anteriormente comentados que se encontraban abiertos.

Esta es la información obtenida con el escaneo sobre el puerto 22 con un servicio ssh:

22/tcp open ssh OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)

| *ssh-hostkey:*

| *1024 af:1c:fb:69:b8:3c:f9:7f:30:ed:0c:e7:53:78:9b:f1 (DSA)*

| *2048 81:21:a8:29:1d:b4:f1:75:c5:65:ff:f7:09:1b:4d:15 (RSA)*

|_ *256 1e:12:b4:b3:56:52:67:48:56:cc:28:c2:df:7a:a3:0d (ECDSA)*

Como podemos ver se han obtenido las claves públicas para los algoritmos criptográficos DSA, RSA y ECDSA en el puerto 22. Hay que destacar que, si bien estas claves son públicas, la amenaza en este caso sería que el atacante pueda conocer qué algoritmo específico de cifrado se está utilizando, y por lo tanto, pueda realizar algún tipo de criptoanálisis.

La siguiente información obtenida está relacionada con el puerto 443, sobre el que escucha un servidor HTTPS para permitir conexiones seguras usando el protocolo SSL:

443/tcp open ssl/http Apache httpd 2.2.22

> *| ssl-cert: Subject: commonName=PFC Javier \xC3\x83\xC3\x83\xC2\x81lvarez Izquierdo/organizationName=PFC-UC3M/stateOrProvinceName=Madrid/countryName=ES*
>
> *| Issuer: commonName=PFC Javier \xC3\x83\xC3\x83\xC2\x81lvarez Izquierdo/organizationName=PFC-UC3M/stateOrProvinceName=Madrid/countryName=ES*
>
> *| Public Key type: rsa*
>
> *| Public Key bits: 1024*
>
> *Device type: general purpose|firewall|storage-misc|WAP|terminal*
>
> *Running (JUST GUESSING): Linux 3.X|2.6.X|2.4.X (95%), IPFire Linux 2.6.X (88%), Iomega Linux 2.6.X (87%), Netgear RAIDiator 4.X (86%), IGEL Linux 2.6.X (85%)*

El análisis sobre el puerto 443 indica que un potencial atacante puede obtener información acerca del certificado utilizado, el tipo, la cantidad de bits utilizados o la versión de cortafuegos utilizada en este puerto. Si bien estos datos son públicos, se puede ver que el certificado utilizado no es oficial (contiene información acerca de un Proyecto de Fin de Carrera, por lo que resulta obvio que es un certificado provisional). Este certificado es propio de un entorno de desarrollo, pero para su implantación en un sistema real de producción, es indispensable obtener un certificado emitido por una Autoridad de Certificación reconocida.

Como complemento a la primera herramienta de escaneo, se utilizó otra herramienta más potente capaz de detectar otro tipo de vulnerabilidades: Nessus.

Al terminar la aplicación el escaneo del sistema mediante Nessus, especificando como objetivo la ip del sistema, se genera un informe sobre las diferentes vulnerabilidades que se habían encontrado en el sistema. Si bien el

informe completo se puede ver en el anexo 2 de esta memoria, las vulnerabilidades detectadas más críticas se comentan a continuación:

1. El servidor web remoto contiene archivos JSP de ejemplo y Servlets instalados por defecto en el contenedor servlet remoto Apache Tomcat/JSP, en estos archivos, además podemos observar fragmentos de código. Concretamente los archivos instalados por defecto son:

   /examples/servlets/index.html
   /examples/jsp/snp/snoop.jsp
   /examples/jsp/index.html

   Estos archivos deben ser eliminados, ya que son innecesarios y pueden facilitar al atacante a revelar información sensible sobre la instalación remota de Tomcat. Asimismo, los propios servicios contenidos en estos ficheros pueden contener otras vulnerabilidades como por ejemplo de tipo cross-site scripting.

   La solución a este problema es revisar los archivos y eliminar aquellos que no sean necesarios.

2. No se puede confiar en el certificado SSL para este servicio, ya que el certificado X.509 del servidor no tiene una firma de una autoridad de certificación pública conocida. Esta situación puede ocurrir de tres maneras diferentes, cada una de las cuales da lugar a una ruptura de la cadena por debajo del cual los certificados no se puede confiar. Primero, la parte superior de la cadena de certificado enviado por el servidor podría no ser descendiente de una entidad de certificación pública conocida. Segundo, la cadena de certificados puede contener un certificado que no es válido en el momento de la exploración. Tercero, la cadena de certificados puede contener una firma que, o bien no coincide con la información del certificado, o podría no ser verificada. Si el host remoto es un sistema público en la producción, que se corte la cadena hace que sea más difícil para los usuarios para verificar la autenticidad y la identidad del servidor web. Esto podría hacer que sea relativamente fácil de llevar a cabo ataques man-in-the-middle contra el host remoto.

3. La cadena de certificados SSL para este servicio termina en un certificado con firma reconocida. La cadena de certificados X.509 para este servicio no está firmado por una autoridad de certificación reconocida. Si la máquina remota es un anfitrión público en la producción, esto anula el uso de SSL como cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.

La solución para estas dos últimas vulnerabilidades sería solicitar o generar un certificado nuevo adecuado para este servicio, emitido por una autoridad reconocida como VerisSing o la Fábrica Nacional de Moneda y Timbre.

4.3. PRUEBAS SEGURIDAD FISICA.

La batería de pruebas para la comprobación de que se cumplan los requisitos de seguridad físicos ha consistido en la realización de visitas periódicas al recinto donde se encuentran alojados los equipos que hacen funcionar la aplicación web.

Las necesidades de seguridad física y lo que realmente se encuentra implantado actualmente se va a representar de la siguiente forma:

Seguridad necesaria	Estado actual
(Seguridad necesaria)	(Estado actual)

Tabla 51: Tabla genérica de pruebas de seguridad física.

(Seguridad necesaria): representa el requisito de seguridad que debería existir.

(Estado actual): como se encuentra en la actualidad.

Como se dijo anteriormente en el presente documento, la aplicación web se encuentra en una máquina virtual en un despacho del departamento de informática de la Universidad Carlos III, al tratarse de un entorno de desarrollo carece de la mayoría de sistemas de seguridad físicos. A continuación se detallaran cuáles son esos sistemas de los que carece:

- Relativas al control de acceso.

Seguridad necesaria	Estado actual
Puertas con cerradura electrónica.	Puerta de madera con cerradura tradicional por llave.

Tabla 52: Prueba de seguridad física Nº 1.

Seguridad necesaria	Estado actual
Código de puerta entregado por encargado de seguridad.	La llave puede entregarla cualquier persona que la tenga del departamento de informática, también la tiene el personal de limpieza.

Tabla 53: Prueba de seguridad física Nº 2.

Seguridad necesaria	Estado actual
Personal de seguridad encargado de la vigilancia.	Posee el que se encarga de la vigilancia de todo el recinto perteneciente a la universidad.

Tabla 54: Prueba de seguridad física Nº 3.

Seguridad necesaria	Estado actual
Circuito cerrado de televisión.	Posee el que se encuentra instalado en la universidad, pero en la sala carece de él.

Tabla 55: Prueba de seguridad física Nº 4.

Seguridad necesaria	Estado actual
Contenedor de seguridad para alojamiento de equipos informáticos.	Carece de cualquier contenedor de seguridad para equipos informáticos, estos se encuentran en las diferentes mesas de la sala.

Tabla 56: Prueba de seguridad física Nº 5.

- Relativas a medidas contra incendios.

Seguridad necesaria	Estado actual
Materiales de la sala resistentes al fuego.	Carece de esos materiales.

Tabla 57: Prueba de seguridad física Nº 6.

Seguridad necesaria	Estado actual
Sistema automático de extinción de incendios por gases.	Carece de sistema automático de extinción de incendios por gases, teniendo uno formado por aspersores de agua.

Tabla 58: Prueba de seguridad física Nº 7.

Seguridad necesaria	Estado actual
Equipos de extinción de incendios portátiles.	La sala carece de ellos, pero si hay en las cercanías.

Tabla 59: Prueba de seguridad física Nº 8.

Seguridad necesaria	Estado actual
Armarios ignífugos para copias de seguridad.	No hay armarios ignífugos en la sala.

Tabla 60: Prueba de seguridad física Nº 9.

Seguridad necesaria	Estado actual
Sistema de aire acondicionado calibrado entre 21 y 23 grados.	Posee el existente en la universidad. No está calibrado entre los 21 y 23 grados.

Tabla 61: Prueba de seguridad física Nº 10.

- Relativas a medidas contra inundaciones.

Seguridad necesaria	Estado actual
Puertas acondicionadas para contener corrientes de agua.	Las puertas son de madera, incapaces de contener corrientes de agua.

Tabla 62: Prueba de seguridad física Nº 11.

Seguridad necesaria	Estado actual
Sistema de interrupción de corriente eléctrica.	Dispone del propio de la universidad.

Tabla 63: Prueba de seguridad física Nº 12.

- Relativas a medidas energéticas.

Seguridad necesaria	Estado actual
Cableado oculto en un falso suelo.	El cableado de los diferentes equipos se encuentra a la vista.

Tabla 64: Prueba de seguridad física Nº 13.

Seguridad necesaria	Estado actual
Sistema de alimentación ininterrumpida.	No existe un sistema de alimentación ininterrumpida propio aunque si está instalado uno genérico que se encuentra en todo el recinto de la universidad que puede utilizarse.

Tabla 65: Prueba de seguridad física Nº 14.

Seguridad necesaria	Estado actual
Servidores auxiliares.	Sólo hay un servidor que de soporte a la aplicación web, en caso de fallo, el sistema entero caería.

Tabla 66: Prueba de seguridad física Nº 15.

4.3.1. Estudio económico de las necesidades para proporcionar seguridad física.

A continuación se van a introducir todos los costes estimados que supondrían adaptar el espacio donde se encuentran los equipos informáticos que dan soporte al sistema para que posean una correcta seguridad física.

Sistema de seguridad	Precio
Puerta con cerradura electrónica	3.000€
Tarjetas electrónicas	2€/ud
Personal de vigilancia	1070,9€/mes (6)
Circuito cerrado de televisión (4 cámaras + videograbador)	1042,85€ (7)
Contenedor de seguridad	103€ (8)
Sala resistente al fuego	4785€ (9)
Extintor portátil	43€/ud
Armario ignífugo	475€
Aire acondicionado	2500€
Falso suelo (1ud= 60x60cm)	85,72€/ud (10)
Servidor web auxiliar	399€

Tabla 67: Estudio económico de seguridad física.

Con este presupuesto económico, acondicionar la sala donde están los equipos que forman el sistema costaría:

Cantidad	Sistema de seguridad	Precio
1	Puerta electrónica	3.000€
2	Tarjetas electrónicas	4€
1	Personal de vigilancia	14.992,6€/año*
1	Circuito de televisión	1042,85€
1	Contenedor de seguridad	103€
1	Sala resistente al fuego	4785€
2	Extintor portátil	86€
1	Armario ignífugo	475€
1	Aire acondicionado	2500€
10	Falso suelo	857,2€
1	Servidor web auxiliar	399€
TOTAL		28.244,65€

Tabla 68: Presupuesto seguridad física.

* 1.070,9 sueldo x 14 pagas = 14.992,6€

5. MEDIDAS A IMPLEMENTAR PARA IMPLANTACION.

En este capítulo se tratarán todas aquellas medidas necesarias de aplicar para que los requisitos establecidos en los capítulos iniciales de la memoria se cumplan adecuadamente. Estas medidas surgen tras el análisis de los resultados de las pruebas realizadas en el capítulo anterior. Para la representación de estas medidas se va a adoptar el siguiente formato:

(Id medida)	Requisito incumplido	Contramedida
	(Requisito)	(Contramedida)

Tabla 69: Tabla genérica de contramedidas.

(Id medida): corresponde con el orden de secuencia de cada medida.

(Requisito): identifica el requisito al que se ajusta la contramedida a adoptar.

(Contramedida): describe la medida a tomar.

Medida Nº 1	Requisito incumplido	Contramedida
Notificación a la AGPD.	RG_1	Para el cumplimiento de este requisito se cumplimentará y presentará en la Agencia Española de Protección de Datos el correspondiente modelo de notificación, utilizando para ello, el medio que le resulte más cómodo: - Programa de ayuda para la generación de notificaciones a través de Internet o mediante soporte magnético (5). - Formularios en soporte papel.

Tabla 70: Medida Nº 1.

Medida Nº2	Requisito incumplido	Contramedida
Deber de secreto.	RG_2	Se incluirá en los contratos de todos los empleados que presten algún servicio para la empresa y que tengan contacto con los datos personales de los pacientes una cláusula por la que deberán guardar el secreto de todos los datos que puedan observar en la realización de sus funciones.

Tabla 71: Medida Nº 2.

Medida Nº 3	Requisito incumplido	Contramedida
Documento de seguridad.	RG_3	Se realizará un documento de seguridad en el que se recogerán las medidas tanto de índole técnica como organizativa que se van a dar para la protección de los datos en la clínica. *Ver anexo 1 "Documento de seguridad".*

Tabla 72: Medida Nº 3.

Medida Nº 4	Requisito incumplido	Contramedida
Consentimiento de los afectados.	RA_1	En el sistema se incluirá una aplicación que, en el momento de dar de alta un nuevo paciente, genere un documento en el que pueda dar, mediante firma física o digital, su consentimiento para el tratamiento de sus datos personales. Además del consentimiento por parte del paciente, el documento debe incluir el tipo de tratamiento que se va a realizar con sus datos, las personas que lo van a realizar e información acerca de los derechos de acceso, rectificación, cancelación y oposición. Cuando se recibe el consentimiento debidamente firmado por el interesado hay que comprobar que la firma es correcta y que proviene de la persona a la que se envió el consentimiento.

Tabla 73: Medida Nº 4.

Medida Nº 5	Requisito incumplido	Contramedida
Usuarios y autorizaciones.	RS_2	En la base de datos se tiene que crear un sistema para que en las tablas donde se guardan los usuarios con sus correspondientes contraseñas, estas se encuentren de forma ininteligible.

Tabla 74: Medida Nº 5.

Medida Nº 6	Requisito incumplido	Contramedida
Control de accesos.	RS_5	Se tiene que incluir en la base de datos los lugares a donde accede cada usuario cuando entra en el sistema.

Tabla 75: Medida Nº 6.

Medida Nº 7	Requisito incumplido	Contramedida
Límite de accesos.	RA_5	Implementar algún método que bloquee a un usuario que intente acceder al sistema en repetidas ocasiones con nombre de usuario y/o contraseñas incorrectas. El límite de accesos será de tres intentos, de lo contrario se bloqueará a ese usuario la entrada al sistema durante un periodo de tiempo de 10min. Cuando sucedan estos intentos de acceso no autorizado al sistema deberá recogerse en un registro de incidencias.

Tabla 76: Medida Nº 7.

Medida Nº 8	Requisito incumplido	Contramedida
Cambio de contraseña.	RA_6	Se creará un sistema que transcurrido un mes del alta de un nuevo usuario mande un recordatorio a este para que cambie su contraseña, este aviso se realizará periódicamente una vez al mes.

Tabla 77: Medida Nº 8.

Medida Nº 9	Requisito incumplido	Contramedida
Canal telemático ARCO.	RA_7	Añadir una opción para los usuarios “paciente” de eliminar su ficha con sus datos personales, o en su defecto un sistema para contactar con los administradores de la aplicación para que se realice la eliminación de los datos personales del afectado.

Tabla 78: Medida Nº 9.

Medida Nº 10	Requisito incumplido	Contramedida
Canal telemático ARCO.	RA_7	Incluir dentro de la aplicación un apartado donde cada usuario pueda mandar incidencias referidas a dudas o funcionamiento de la aplicación. Serán recogidas en un archivo para tener un registro de todos los problemas que pueden aparecer en la aplicación.

Tabla 79: Medida Nº 10.

Medida Nº 11	Requisito incumplido	Contramedida
Eliminación de datos no viables.	RS_7	En el sistema se implementará un gestor de bajas de los usuarios que deseen eliminarse del sistema, este sistema cuando se realice la baja de dicho usuario debe, además de dar de baja el usuario para la entrada al sistema, eliminar todos los datos que estuvieran relacionados con dicho usuario. Sería conveniente que esto sólo lo pudiera realizar el personal administrador del sistema bajo petición del usuario que desea darse de baja.

Tabla 80: Medida Nº 11.

Medida Nº 12	Requisito incumplido	Contramedida
Gestión de documentos y soportes.	RA_9	Añadir un gestor que controle toda la documentación que genera la aplicación (consentimientos, pruebas médicas, resultados…), además de incluir un registro con los soportes que forman el sistema.

Tabla 81: Medida Nº 12.

Medida Nº 13	Requisito incumplido	Contramedida
Copias de respaldo.	RA_10	Se creará de forma paralela un sistema de backup para la generación de copias de respaldo y recuperación en caso de pérdida o destrucción, estas copias se realizarán cada semana de forma periódica y serán revisados semestralmente los procedimientos de copia.

Tabla 82: Medida Nº 13.

Medida Nº 14	Requisito incumplido	Contramedida
Verificación firma digital.	RA_3	Mediante la plataforma @firma se podrá verificar la firma de los documentos de cada paciente.

Tabla 83: Medida Nº 14.

Medida Nº 15	Requisito incumplido	Contramedida
Verificación certificado digital.	RA_4	Mediante la plataforma @firma se podrá verificar el certificado de los documentos de cada paciente.

Tabla 84: Medida Nº 15.

6. PRESUPUESTO DEL PROYECTO.

Auditoría sobre aplicación web para la gestión de una clínica de reproducción asistida.

1/ Autor:

Ricardo Ramírez de Antón Molina.

2/ Departamento:

Departamento de informática.

3/ Descripción del proyecto:

- Título: Auditoría sobre aplicación web para la gestión de una clínica de reproducción asistida.
- Duración (Meses): 6.
- Tasas de costes indirectos: 10%.

4/ Presupuesto total del proyecto:

19.190,47 €

5/ Desglose presupuestario (costes indirectos):

Personal.

Apellidos y nombre	Categoría	Dedicación (hombres mes)	Coste hombres mes [I)]	Coste
Pastrana Portillo, Sergio	Ingeniero Sénior	0,25	4.289,54	1.072,335€
Ramírez de Antón Molina, Ricardo	Ingeniero Junior	6	2.694,39	16.166,16€
			Total	**17.238,50€**

Tabla 85: Desglose presupuestario - Personal.

I) 1 Hombre mes = 131,25 horas. Máximo anual de dedicación de 12 hombres mes (1.575 horas).

Máximo anual para PDI de la Universidad Carlos III de Madrid de 8,8 hombres mes (1.155 horas).

Equipos.

Descripción	Coste	% Uso dedicado al proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable II)
Acer Aspire 5750G	699	100	6	48 meses	87,38€
				Total	**87,38€**

Tabla 86: Desglose presupuestario – Equipos.

II) Fórmula de cálculo de la Amortización.

$$\frac{A}{B} \times C \times D$$

A = nº de meses desde la fecha de facturación en que el equipo es utilizado.
B = Periodo de deprecación (48 meses)
C = coste del equipo (sin IVA)
D = % del uso que se dedica al proyecto.

Otros costes.

Descripción	Coste	Cantidad	Coste imputable
Dietas y transporte	30	4	120€
		Total	**120€**

Tabla 87: Desglose presupuestario - Otros costes.

6/ Resumen de costes:

Presupuesto	Costes
Personal	17.238,50€
Amortización	87,38€
Otros costes	120€
Costes indirectos	1.744,59€
Total	**19.191€**

Tabla 88: Resumen de costes.

“El presupuesto total de este proyecto asciende a la cantidad de DIECINUEVEMIL CIENTONOVENTA Y UN EUROS”.

Leganés a 10 de Julio de 2014.

El ingeniero proyectista

Fdo. Ricardo Ramírez de Antón Molina.

7. CONCLUSIONES Y LÍNEAS FUTURAS.

7.1. Conclusiones.

El objetivo del presente proyecto es desarrollar una auditoría de una aplicación web en la que se realiza tratamiento de datos personales para comprobar si en el momento de desarrollar dicha aplicación se tuvieron en cuenta todos los aspectos legales que rigen las leyes de protección de datos personales en nuestro país. Este objetivo se ha cumplido satisfactoriamente gracias a la creación de una auditoría donde se han detectado todas las deficiencias relacionadas con el incumplimiento de la legislación vigente y se han suministrado una serie de medidas para subsanar todas ellas.

La auditoría examina cada una de las obligaciones legales recogidas en el análisis de requisitos mediante diferentes pruebas y propone las soluciones a todos aquellos que en las pruebas se determinan que no están correctamente aplicados.

Debido a que el personal que pueda tratar el informe detallado en esta auditoría es posible que no sea un experto en derecho se señalan las partes concretas que la aplicación web vulnera en estos momentos, el tipo de sanciones y su cuantía conforme dicta la ley, las soluciones a todos aquellos problemas que se han detectado por requisitos legales no cumplimentados. Además se adjunta un estudio económico de las medidas físicas que se deberían adoptar, las lógicas al intervenir multitud de factores no se ha realizado ninguno.

Con este proyecto académico se ha demostrado la necesidad de considerar los requisitos de seguridad en las fases iniciales de desarrollo de cualquier producto software (como la aplicación web estudiada). De hecho, el conjunto elevado de medidas a desarrollar a posteriori en la aplicación (para que esta cumpla con la LOPD) conlleva a la realización de un esfuerzo extra (tanto económico como de recursos operacionales). Este esfuerzo podría suponer grandes pérdidas económicas para cualquier empresa, muchas veces no asumibles en los tiempos de desavenencias económicas que corren.

7.3. Conclusiones personales.

La creación de una aplicación para gestionar cualquier dato personal conlleva una gran cantidad de trabajo tanto en el transcurso de desarrollo de la propia aplicación como posterior realizando gran cantidad de controles legales. La elaboración de este proyecto me ha permitido observar en continuo control que se debe realizar a proyectos ya terminados para evitar que se reciban fuertes sanciones por incumplimiento de las leyes de nuestro país.

En el transcurso del proyecto he estado involucrado en todas las fases del avance de la auditoría, personalmente para mí las más significativas han sido:

Definición de unos objetivos.

El estudio de una legislación no conocida hasta ahora.

La creación de una serie de requisitos en los que basar las líneas de actuación del proyecto.

El manejo de tecnologías para realizar estudios de seguridad.

7.2. Líneas futuras.

Cómo se apuntó en el apartado 1.2. Motivación, el proyecto está encuadrado en un conjunto de proyectos que componen un proyecto global. Por lo tanto, el siguiente paso a seguir a raíz de este tercer proyecto serían la subsanación de todos aquellos problemas detectados por la auditoría para que la aplicación web pueda salir del entorno de desarrollo, y una vez conseguido eso seguir con la finalidad del proyecto principal, crear un sistema de ayuda a la toma de decisiones en la selección de embriones.

Paralelamente a la creación de este proyecto para la toma de decisiones, sería conveniente realizar una revisión a la auditoría realizada en este proyecto actual para así corroborar que las directrices expuestas en él han sido tomadas en cuenta y todos los errores que provocan que se generen infracciones legales sean subsanados correctamente.

Como finiquito al proyecto global sería conveniente realizar una nueva auditoría de seguridad al sistema de ayuda a la toma de decisiones, que englobaría todos los proyectos anteriores, para comprobar que cumple correctamente con toda la legislación vigente sobre protección de datos al tratarse ya de un producto final y poder abandonar el estado de desarrollo en el que se encuentra actualmente.

8. REFERENCIAS BIBLIOGRÁFICAS.

Bibliografía

1. (s.f.). Obtenido de Asesoría para pymes: http://consultingintegral.es/incumplimiento-de-la-lopd/

2. (21 de Junio de 2012). Obtenido de Marco legal y tecnológico para la gestión de datos clínicos: http://e-archivo.uc3m.es/handle/10016/15732

3. (12 de Febrero de 2014). *Aplicación web para la gestión de datos clínicos relativos a los servicios de reproducción asistida humana.*

4. (s.f.). Obtenido de Agencia Española de Proteccion de Datos: http://www.servicios.agpd.es/Evalua/home.seam

5. (s.f.). Obtenido de Agencia Española de Protección de Datos. : https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/Notificaciones_tele/index-ides-idphp.php

6. (s.f.). Obtenido de Seguridad Privada: http://www.seguridad-privada.net/seguridad-privada-salario.html

7. (s.f.). Obtenido de Tu antena: http://www.tuantena.com/categories.php?category=CAMARAS-DE-VIGILANCIA/KITS-CIRCUITO-CERRADO-TV

8. (s.f.). Obtenido de pc componentes: http://www.pccomponentes.com/armarios_rack.html

9. (s.f.). Obtenido de mieapq: http://www.mieapq.com/index.php?cPath=21

10. (s.f.). Obtenido de Generador de precios: http://www.generadordeprecios.info/obra_nueva/Revestimientos/Suelos_y_pavimentos/Tecnicos/Suelo_tecnico_registrable.html

Anexo I: Documento de Seguridad.

Documento de seguridad de datos.

Agencia Española de Protección de Datos.

Ricardo Ramírez de Antón Molina.

El Real Decreto 1720/2007,de 21 de diciembre, desarrolla las distintas medidas de seguridad en el tratamiento de datos personales. Una de estas medidas es la creación de un documento de seguridad donde se recogen todas las medidas a adoptar.

1. Introducción.

Según el Real Decreto 1720/2007 de 21 de diciembre, título VIII, capítulo II, artículo 88 se recoge:

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:

    a. Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
    b. Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.
    c. Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
    d. Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
    e. Procedimiento de notificación, gestión y respuesta ante las incidencias.
    f. Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
    g. Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

    a. La identificación del responsable o responsables de seguridad.
    b. Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados. En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

2. Ámbito de aplicación del documento.

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de Ricardo Ramírez de Antón Molina, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican. En concreto, los ficheros sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente, son los siguientes:

- Base de Datos de la clínica REPROFIV con un nivel de seguridad alto al tratar un tema relacionado con la salud o la vida sexual.

3. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.

3.1. Identificación y autenticación.

Medidas y normas relativas a la identificación y autenticación del personal autorizado para acceder a los datos personales.

El administrador del sistema realizará el alta/registro de las personas que podrán acceder al sistema, creará un login al usuario y una contraseña generada automáticamente y que se deberá cambiar la primera vez que el usuario acceda al sistema, formándose esta obligatoriamente por letras (mayúsculas y minúsculas) y al menos un número o carácter especial. Dichas contraseñas se almacenarán de forma ininteligible y deberán cambiarse al menos una vez cada año.

Los usuarios tendrán un límite de tres intentos para introducir correctamente el usuario asignado junto con la respectiva contraseña. De superarse esos tres intentos la cuenta quedará bloqueada y deberá contactar con el administrador del sistema para poder restaurarla de nuevo.

3.2. Control de accesos.

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados mediante un sistema de roles o permisos.

Exclusivamente el administrador del sistema está autorizado para conceder, alterar o anular el acceso sobre los datos y los recursos, conforme a los criterios establecidos por el responsable del fichero.

Para solicitar el alta o baja de las autorizaciones de acceso a los datos hay que dirigirse directamente al administrador del sistema para que los realice, por otro lado cada usuario podrá modificar únicamente la contraseña que desea utilizar, la modificación de las funciones que puede realizar en el sistema (roles) solo puede modificarlos el administrador.

De existir personal ajeno al responsable del fichero con acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

3.3. Registro de accesos.

En los accesos a los datos de los ficheros de nivel alto, se registrará por cada acceso la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. Si el acceso fue autorizado, se almacenará también la información que permita identificar el registro accedido.

Los datos del registro de accesos se conservaran durante un mínimo de dos años. Una vez sobrepasado ese tiempo podrán ser eliminados a elección de la entidad.

El responsable de seguridad revisará al menos una vez al mes la información de control registrada y elaborará un informe según se detalla en el capítulo de “Comprobaciones para la realización de la auditoría de seguridad” de este documento.

3.4. Gestión de soportes y documentos.

Los soportes que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y serán almacenados en el centro informático, lugar de acceso restringido al que solo tendrán acceso las personas con autorización que se relacionan a continuación: responsable de seguridad y administrador del sistema, para permitir el acceso a otra persona, este permiso debe ser dado por cualquiera de los dos responsables anteriores y siempre que en las funciones de la nueva persona autorizada estén la manipulación de datos del sistema (introducción, modificación, actualización, borrado…) o mantenimiento de los equipos que forman el sistema de información. En el momento en el que estas personas dejen de realizar las funciones citadas será obligación del responsable de seguridad o administrador del sistema retirar el permiso de acceso.

Los siguientes soportes, formularios (en formato papel), se exceptúan de las obligaciones indicadas en el párrafo anterior, dadas sus características físicas, que imposibilitan el cumplimiento de las mismas.

Los soportes que vayan a ser desechados, deberán ser previamente comprobados que en ellos no existe información, toda debe ser borrada y los discos duros que pudieran tener información deben quedar vacíos de información de forma que no sea posible el acceso a la información contenida en ellos o su recuperación posterior.

En el traslado de la documentación se adoptarán las siguientes medidas para evitar la sustracción, pérdida o acceso indebido a la información: una vez trasladada la información al sistema informático, la documentación de los pacientes será trasladada hasta el centro informático donde se guardarán en una serie de archivadores que allí se encuentran.

3.5. Registro de entrada y salida de soportes.

El registro de entrada y salida de soportes se gestionará mediante un registro de soportes y en el que deberán constar: tipo de soporte, fecha y hora, emisor, numero de soportes, información que contiene, forma de envío y persona responsable.

Este registro de soportes se realizará de forma automatizada (base de datos) y se guardarán todas las entradas y salidas de los soportes para tener un control de todos ellos. En esta base de datos además se tendrá información sobre dichos soportes como: tipo de soporte, número de serie, tipo de software (en caso de tener), tipo de hardware (en caso de tener), información que contiene.

3.6. Ficheros temporales o copias de trabajo de documentos.

Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de medidas de seguridad, y serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

3.7. Copias de respaldo y recuperación.

Se realizarán copias de respaldo, salvo que no se hubiese producido ninguna actualización de los datos, con la siguiente periodicidad una vez a la semana se realizará una copia gradual (solo se guardarán los últimos 7 días) y una vez al mes se realizara una copia completa de todo lo realizado en ese mes.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. En el caso de los ficheros parcialmente automatizados siguientes formularios en formato papel se grabarán manualmente los datos.

El responsable del fichero verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.

Las pruebas anteriores a la implantación o modificación de sistemas de información se realizarán con datos reales previa copia de seguridad, y garantizando el nivel correspondiente al tratamiento realizado.

En los ficheros de nivel alto se conservará una copia de respaldo y de los procedimientos de recuperación de los datos en despacho del administrador del sistema.

3.8. Responsable de seguridad.

Se designa como responsable de seguridad que con carácter general se encargará de coordinar y controlar las medidas definidas en este documento de seguridad.

En ningún caso, la designación supone una exoneración de la responsabilidad que corresponde al administrador del sistema como responsable del fichero de acuerdo con el RLOPD.

El responsable de seguridad desempeñará las funciones encomendadas durante el periodo de un año. Una vez transcurrido este plazo el administrador del sistema podrá nombrar al mismo responsable de seguridad o a otro diferente.

4. INFORMACIÓN Y OBLIGACIONES DEL PERSONAL

4.1. Información al personal.

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo con el siguiente procedimiento: curso informativo obligatorio sobre el cumplimiento de la RLOPD donde se le explicarán todas las normas que se deben cumplir y las consecuencias que acarrean el no obedecer estas normas. Todos los empleados que reciban este curso deberán firmar un documento en el que diga que se les ha informado sobre las normas que se recogen en la ley.

4.2. Funciones y obligaciones del personal.

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Constituye una obligación del personal notificar al administrador del sistema o responsable de seguridad las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este Documento, y en concreto en el apartado de “Procedimientos de notificación, gestión y respuesta ante las incidencias.”

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

El personal que realice trabajos que no impliquen el tratamiento de datos personales tendrán limitado el acceso a estos datos, a los soportes que los contengan, o a los recursos del sistema de información.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto de aquellos datos que hubiera podido conocer durante la prestación del servicio.

4.3. Consecuencias del incumplimiento del documento de seguridad.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado, se sancionará conforme a RLOPD.

Son infracciones leves: sanciones entre 900 € y 40.000 €

- No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo.
- No solicitar la inscripción del fichero en el Registro General de Protección de Datos.
- Recopilar datos personales sin informar previamente.
- No atender a las solicitudes de rectificación o cancelación.
- Transmitir datos a un encargado de tratamiento sin cumplir las obligaciones formales.

Son infracciones graves: sanciones entre 40.001 € y 300.000 €

- No inscribir los ficheros en la AEPD.
- Utilizar los ficheros con finalidad distinta con la se crearon.
- No tener el consentimiento del interesado para recabar sus datos personales.
- No permitir el acceso a los ficheros.
- Mantener datos inexactos o no efectuar las modificaciones solicitadas.
- No seguir los principios y garantías de la LOPD.
- Tratar datos especialmente protegidos sin la autorización del afectado.
- No remitir a la AGPD las notificaciones previstas en la LOPD.
- Mantener los ficheros sin las debidas condiciones de seguridad.

Son infracciones muy graves: sanciones entre 300.001 € y 600.000 €

- Crear ficheros para almacenar datos especialmente protegidos.
- Recogida de datos con engañoso o fraudulentamente.
- Recabar datos especialmente protegidos sin la autorización del afectado.
- No atender u obstaculizar de forma sistemática las solicitudes de cancelación o rectificación.
- Vulnerar el secreto sobre datos especialmente protegidos.
- La comunicación o cesión de datos cuando ésta no esté permitida.
- No cesar en el uso ilegítimo a petición de la AEPD.
- Tratar los datos de forma ilegítima o con menosprecio de principios y garantías que le sean de aplicación.
- No atender de forma sistemática los requerimientos de la AEPD.
- La transferencia temporal o definitiva de datos de carácter. personal con destino a países sin nivel de protección equiparable o sin autorización.

5. PROCEDIMIENTOS DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS.

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal del administrador del sistema.

El procedimiento a seguir para la notificación de incidencias será comunicar personalmente o mediante correo electrónico al administrador del sistema o responsable de seguridad (preferiblemente por correo para dejar constancia).

El registro de incidencias se gestionará informáticamente, en el registro aparecerá el tipo de incidencia, fecha y hora, persona que realiza la incidencia, persona a la que se dirige, efectos que produce la incidencia y su solución. Esta gestión se realizará mediante un gestor de correos electrónicas localizado en una intranet.

En el registro de incidencias se consignarán también los procedimientos de recuperación de datos que afecten a los ficheros de nivel medio y alto, del modo que se indica a continuación: se deberá crear una incidencia con el título “recuperación de datos + fecha” en que se incluirá la persona que ejecutó el proceso, los datos restaurados y, en su caso, que datos ha sido necesario grabar manualmente en el proceso de recuperación.

Para ejecutar los procedimientos de recuperación de datos en los ficheros mencionados en el párrafo anterior, será necesaria la autorización por escrito del responsable del fichero.

6. PROCEDIMIENTOS DE REVISIÓN.

6.1. Revisión del documento de seguridad.

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en el contenido de la información incluida en los ficheros o como consecuencia de los controles periódicos realizados. En todo caso se entenderá como cambio relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas. Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

En el caso de que el documento de seguridad deba ser actualizado, el responsable de seguridad deberá crear una incidencia titulada “Actualización documento de seguridad” en la que aparecerá las modificaciones que son necesarias realizar, luego se sustituirá el documento por el nuevo actualizado y si alguna persona se viera afectado por las modificaciones se le remitirá una copia del nuevo documento señalando que parte le afecta.

6.2. Auditoría.

Cada dos años deberá realizarse una auditoría ya sea interna o externa en la que se garanticen que el sistema cumple debidamente con las medidas de seguridad recogidas en la RLOPD.

Con carácter extraordinario deberán realizarse auditorias cuando se lleven a cabo modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas, con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado.

El informe analizará la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificará las deficiencias y propondrá las medidas correctoras o complementarias necesarias.

Los informes de auditoría han de ser analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras y quedará a disposición de la Agencia

Española de Protección de Datos, o en su caso de las autoridades de control de las comunidades autónomas.

6.3. Informe mensual sobre el registro de accesos.

En el registro de accesos a los datos del sistema se guardará:

- Usuario.
- Fecha y hora.
- Fichero al que se accede.
- Tipo de acceso.
- Autorizado o denegado.

Si el acceso a los datos ha sido autorizado se guardará la información que permite identificar el registro al que se accede. Todos estos datos registrados se guardarán un mínimo de dos años.
Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y será el encargado de realizar este informe mensual señalando en el los distintos problemas detectados en el sistema.

Anexo II: Escaneo de vulnerabilidades.

163.117.149.128

Summary

Critical	High	Medium	Low	Info	Total
0	0	3	4	26	33

163.117.149.128

Scan Information

Start time: Thu May 22 16:49:31 2014

End time: Thu May 22 16:53:40 2014

Host Information

IP: 163.117.149.128

OS: Linux Kernel 3.0 on Ubuntu 12.04 (precise)

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	4	4	38	46

Results Details

12085 (2) - Apache Tomcat servlet/JSP container default files

Synopsis

The remote web server contains example files.

Description

Example JSPs and Servlets are installed in the remote Apache Tomcat servlet/JSP container. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself. Or they may themselves contain vulnerabilities such as cross-site scripting issues.

Solution

Review the files and delete those that are not needed.

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

Plugin Information:

Publication date: 2004/03/02, Modification date: 2012/01/20

Hosts

163.117.149.128 (tcp/443)

```
The following default files were found :

/examples/servlets/index.html
/examples/jsp/snp/snoop.jsp
/examples/jsp/index.html
```

163.117.149.128 (tcp/8080)

```
The following default files were found :

/examples/servlets/index.html
/examples/jsp/snp/snoop.jsp
/examples/jsp/index.html
```

51192 (1) - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.

First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2010/12/15, Modification date: 2014/02/27

Hosts

163.117.149.128 (tcp/443)

```
The following certificate was at the top of the certificate
chain sent by the remote host, but is signed by an unknown
certificate authority :
```

```
|-Subject : C=ES/ST=Madrid/L=Madrid/O=PFC-UC3M/OU=UC3M/CN=PFC Javier
......lvarez Izquierdo/E=javier.alvarez.izquierdo@gmail.com
|-Issuer : C=ES/ST=Madrid/L=Madrid/O=PFC-UC3M/OU=UC3M/CN=PFC Javier
......lvarez Izquierdo/E=javier.alvarez.izquierdo@gmail.com
```

57582 (1) - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2012/01/17, Modification date: 2012/10/25

Hosts

163.117.149.128 (tcp/443)

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=ES/ST=Madrid/L=Madrid/O=PFC-UC3M/OU=UC3M/CN=PFC Javier
......lvarez Izquierdo/E=javier.alvarez.izquierdo@gmail.com
```

65821 (1) - SSL RC4 Cipher Suites Supported

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g. HTTP cookies), and an attacker is able to obtain many (i.e. tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.nessus.org/u?217a3666

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

2.3 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

BID	58796
CVE	CVE-2013-2566
XREF	OSVDB:91162

Plugin Information:

Publication date: 2013/04/05, Modification date: 2014/02/27

Hosts

163.117.149.128 (tcp/443)

```
Here is the list of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

SSLv3
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

TLSv1
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

69551 (1) - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Synopsis

The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.

Description

At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits.

Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.

Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

See Also

https://www.cabforum.org/Baseline_Requirements_V1.pdf

Solution

Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

Risk Factor

Low

Plugin Information:

Publication date: 2013/09/03, Modification date: 2014/04/10

Hosts

163.117.149.128 (tcp/443)

```
The following certificates were part of the certificate chain
sent by the remote host, but contain RSA keys that are considered
to be weak :

|-Subject : C=ES/ST=Madrid/L=Madrid/O=PFC-UC3M/OU=UC3M/CN=PFC Javier
......lvarez Izquierdo/E=javier.alvarez.izquierdo@gmail.com
|-RSA Key Length : 1024 bits
```

70658 (1) - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

2.3 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

BID	32319
CVE	CVE-2008-5161
XREF	OSVDB:50035
XREF	OSVDB:50036
XREF	CERT:958563
XREF	CWE:200

Plugin Information:

Publication date: 2013/10/28, Modification date: 2014/01/28

Hosts

163.117.149.128 (tcp/22)

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

71049 (1) - SSH Weak MAC Algorithms Enabled

Synopsis

SSH is configured to allow MD5 and 96-bit MAC algorithms.

Description

The SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2013/11/22, Modification date: 2013/11/23

Hosts

163.117.149.128 (tcp/22)

```
The following client-to-server Method Authentication Code (MAC)
algorithms
are supported :

hmac-md5
hmac-md5-96
hmac-sha1-96
hmac-sha2-256-96
hmac-sha2-512-96

The following server-to-client Method Authentication Code (MAC)
algorithms
are supported :

hmac-md5
hmac-md5-96
hmac-sha1-96
hmac-sha2-256-96
hmac-sha2-512-96
```

11219 (5) - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2014/01/23

Hosts

163.117.149.128 (tcp/22)

```
Port 22/tcp was found to be open
```

163.117.149.128 (tcp/80)

```
Port 80/tcp was found to be open
```

163.117.149.128 (tcp/443)

```
Port 443/tcp was found to be open
```

163.117.149.128 (tcp/8009)

```
Port 8009/tcp was found to be open
```

163.117.149.128 (tcp/8080)

```
Port 8080/tcp was found to be open
```

22964 (5) - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2014/05/09

Hosts

163.117.149.128 (tcp/22)

```
An SSH server is running on this port.
```

163.117.149.128 (tcp/80)

```
A web server is running on this port.
```

163.117.149.128 (tcp/443)

```
A TLSv1 server answered on this port.
```

163.117.149.128 (tcp/443)

```
A web server is running on this port through TLSv1.
```

163.117.149.128 (tcp/8080)

```
A web server is running on this port.
```

10107 (3) - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2014/04/07

Hosts

163.117.149.128 (tcp/80)

```
The remote web server type is :

Apache/2.2.22 (Ubuntu)

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.
```

163.117.149.128 (tcp/443)

```
The remote web server type is :

localhost
```

163.117.149.128 (tcp/8080)

```
The remote web server type is :

localhost
```

24260 (3) - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

Hosts

163.117.149.128 (tcp/80)

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Thu, 22 May 2014 14:52:30 GMT
Server: Apache/2.2.22 (Ubuntu)
Location: https://163.117.149.128/
Vary: Accept-Encoding
Content-Length: 313
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

163.117.149.128 (tcp/443)

```
Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Thu, 22 May 2014 14:52:30 GMT
Server: localhost
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

163.117.149.128 (tcp/8080)

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Content-Length: 0
Date: Thu, 22 May 2014 14:52:30 GMT
Connection: close
Server: localhost
```

10114 (1) - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Hosts

163.117.149.128 (icmp/0)

```
The difference between the local and remote clocks is -2 seconds.
```

10267 (1) - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2011/10/24

Hosts

163.117.149.128 (tcp/22)

```
SSH version : SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.1
SSH supported authentication : publickey,password
```

10287 (1) - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2013/04/11

Hosts

163.117.149.128 (udp/0)

```
For your information, here is the traceroute from 192.168.1.10 to
163.117.149.128 :
```

192.168.1.10
192.168.1.1
10.212.32.1
10.127.45.85
10.207.243.57
10.254.5.110
80.239.160.133
62.115.38.186
4.69.201.226
4.69.141.58
4.69.158.186
4.69.141.45
213.242.113.78
130.206.245.1
130.206.212.94
193.145.14.129
193.145.14.21
163.117.49.4
163.117.149.128

10386 (1) - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/04/28, Modification date: 2014/04/25

Hosts

163.117.149.128 (tcp/80)

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 301
rather than 404. The requested URL was :

http://163.117.149.128/C0zBC_yn006g.html
```

10863 (1) - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/05/19, Modification date: 2012/04/02

Hosts

163.117.149.128 (tcp/443)

```
Subject Name:

Country: ES
State/Province: Madrid
Locality: Madrid
Organization: PFC-UC3M
Organization Unit: UC3M
Common Name: PFC Javier ......lvarez Izquierdo
Email Address: javier.alvarez.izquierdo@gmail.com

Issuer Name:

Country: ES
State/Province: Madrid
Locality: Madrid
```

```
Organization: PFC-UC3M
Organization Unit: UC3M
Common Name: PFC Javier ......lvarez Izquierdo
Email Address: javier.alvarez.izquierdo@gmail.com

Serial Number: 00 FE 0A 10 35 B2 76 19 53

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 26 11:05:17 2013 GMT
Not Valid After: Oct 26 11:05:17 2014 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 B3 61 22 BE 79 72 75 EA 85 A0 15 12 09 54 D1 CB 03 EE
61
8C 36 1B 5F 2E 63 08 42 CD 1F 81 05 D9 EB D4 83 E6 72 98 F2
91 03 E0 75 71 48 BA DA F7 76 62 FA 6A 09 5B 78 9A 67 F4 D7
85 7D 5A 13 23 4D A3 2B 1F 0D CC AE AA 07 35 69 9C C4 81 55
7C D7 0F F6 7B E1 56 B2 26 A1 FB D1 F3 11 97 65 FF 71 98 0F
0F 42 BE 95 A3 E5 5A BD 9A 28 32 83 62 8C F8 4E 8A 53 C0 77
93 3E 49 47 02 D4 4A ED 99
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 5A 78 70 7F B7 A7 AD 1A B0 3A 4F 65 E7 90 DF 0A 8C A9 C6
76 84 87 F9 17 86 17 F1 B9 5F 94 91 8B ED C8 8D E2 22 DD E7
7B 6C 6C 0D A5 C2 D2 4C A3 71 B8 4C 01 B7 71 1A 69 79 5B 70
71 B4 B0 BB E3 6E CA 84 07 64 7C A5 19 76 B8 6C E3 4A 62 62
44 59 C3 9B D0 E3 A7 24 18 8D 04 AD 0A D8 D0 64 00 21 12 61
F3 03 FE A3 C8 7A CA 45 FE 58 75 B1 21 94 A8 D4 F6 02 CF D3
61 B4 A4 5B 7C 74 BB F3 0B
```

11936 (1) - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...), it is possible to guess the name of the remote operating system in use. It is also sometimes possible to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2014/02/19

Hosts

163.117.149.128 (tcp/0)

```
Remote operating system : Linux Kernel 3.0 on Ubuntu 12.04 (precise)
Confidence Level : 95
Method : SSH


The remote host is running Linux Kernel 3.0 on Ubuntu 12.04 (precise)
```

18261 (1) - Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

This script extracts the banner of the Apache web server and attempts to determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit httpd.conf and set the directive 'ServerTokens Prod' and restart Apache.

Risk Factor

None

Plugin Information:

Publication date: 2005/05/15, Modification date: 2014/03/17

Hosts

163.117.149.128 (tcp/0)

```
The linux distribution detected was :
- Ubuntu 12.04 (precise)
- Ubuntu 12.10 (quantal)
- Ubuntu 13.04 (raring)
```

19506 (1) - Nessus Scan Information

Synopsis

Information about the Nessus scan.

Description

This script displays, for each tested host, information about the scan itself :

- The version of the plugin set
- The type of scanner (Nessus or Nessus Home)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management checks are possible
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2014/04/07

Hosts

163.117.149.128 (tcp/0)

```
Information about this scan :

Nessus version : 5.2.1 (Nessus 5.2.6 is available - consider
upgrading)
```

```
Plugin feed version : 201405220415
Scanner edition used : Nessus Home
Scan policy used : pfc
Scanner IP : 192.168.1.10
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2014/5/22 16:49
Scan duration : 245 sec
```

21186 (1) - AJP Connector Detection

Synopsis

There is an AJP connector listening on the remote host.

Description

The remote host is running an AJP (Apache JServ Protocol) connector, a service by which a standalone web server such as Apache communicates over TCP with a Java servlet container such as Tomcat.

See Also

http://tomcat.apache.org/connectors-doc/

http://tomcat.apache.org/connectors-doc/ajp/ajpv13a.html

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/04/05, Modification date: 2011/03/11

Hosts

163.117.149.128 (tcp/8009)

```
The connector listing on this port supports the ajp13 protocol.
```

21643 (1) - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This script detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

http://www.openssl.org/docs/apps/ciphers.html

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2014/01/15

Hosts

163.117.149.128 (tcp/443)

```
Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
```

```
SSLv3
EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

TLSv1
EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES-CBC(168) Mac=SHA1
DHE-RSA-AES128-SHA Kx=DH Au=RSA Enc=AES-CBC(128) Mac=SHA1
DHE-RSA-AES256-SHA Kx=DH Au=RSA Enc=AES-CBC(256) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA Kx=DH Au=RSA Enc=Camellia-CBC(128) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA Kx=DH Au=RSA Enc=Camellia-CBC(256) Mac=SHA1
DHE-RSA-SEED-SHA Kx=DH Au=RSA Enc=SEED-CBC(128) Mac=SHA1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA1
CAMELLIA128-SHA Kx=RSA Au=RSA Enc=Camellia-CBC(128) Mac=SHA1
CAMELLIA256-SHA Kx=RSA Au=RSA Enc=Camellia-CBC(256) Mac=SHA1
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
SEED-SHA Kx=RSA Au=RSA Enc=SEED-CBC(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

25220 (1) - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Hosts

163.117.149.128 (tcp/0)

39520 (1) - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

http://www.nessus.org/u?d636c8c7

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/06/25, Modification date: 2013/04/03

Hosts

163.117.149.128 (tcp/22)

```
Give Nessus credentials to perform local checks.
```

39521 (1) - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

http://www.nessus.org/u?d636c8c7

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/06/25, Modification date: 2013/10/02

Hosts

163.117.149.128 (tcp/80)

```
Give Nessus credentials to perform local checks.
```

45590 (1) - Common Platform Enumeration (CPE)

Synopsis

It is possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2014/05/15

Hosts

163.117.149.128 (tcp/0)

```
The remote operating system matched the following CPE :

cpe:/o:canonical:ubuntu_linux:12.04

Following application CPE's matched on the remote system :

cpe:/a:openbsd:openssh:5.9 -> OpenBSD OpenSSH 5.9
cpe:/a:apache:http_server:2.2.22 -> Apache Software Foundation Apache
HTTP Server 2.2.22
```

50845 (1) - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

http://www.openssl.org

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/11/30, Modification date: 2013/10/18

Hosts

163.117.149.128 (tcp/443)

51891 (1) - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/02/07, Modification date: 2013/10/18

Hosts

163.117.149.128 (tcp/443)

```
This port supports resuming SSLv3 sessions.
```

54615 (1) - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Hosts

163.117.149.128 (tcp/0)

```
Remote device type : general-purpose
Confidence level : 95
```

56984 (1) - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This script detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/01, Modification date: 2014/04/14

Hosts

163.117.149.128 (tcp/443)

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

57041 (1) - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

http://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/07, Modification date: 2012/04/02

Hosts

163.117.149.128 (tcp/443)

```
Here is the list of SSL PFS ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

SSLv3
EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1

TLSv1
EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES-CBC(168) Mac=SHA1
DHE-RSA-AES128-SHA Kx=DH Au=RSA Enc=AES-CBC(128) Mac=SHA1
DHE-RSA-AES256-SHA Kx=DH Au=RSA Enc=AES-CBC(256) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA Kx=DH Au=RSA Enc=Camellia-CBC(128) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA Kx=DH Au=RSA Enc=Camellia-CBC(256) Mac=SHA1
DHE-RSA-SEED-SHA Kx=DH Au=RSA Enc=SEED-CBC(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

62563 (1) - SSL Compression Methods Supported

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml

http://tools.ietf.org/html/rfc3749

http://tools.ietf.org/html/rfc3943

http://tools.ietf.org/html/rfc5246

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/10/16, Modification date: 2013/10/18

Hosts

163.117.149.128 (tcp/443)

```
Nessus was able to confirm that the following compression method is
supported by the target :

NULL (0x00)
```

70544 (1) - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://www.nessus.org/u?cc4a822a

http://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/22, Modification date: 2013/10/22

Hosts

163.117.149.128 (tcp/443)

```
Here is the list of SSL CBC ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

TLSv1
EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES-CBC(168) Mac=SHA1
DHE-RSA-AES128-SHA Kx=DH Au=RSA Enc=AES-CBC(128) Mac=SHA1
DHE-RSA-AES256-SHA Kx=DH Au=RSA Enc=AES-CBC(256) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA Kx=DH Au=RSA Enc=Camellia-CBC(128) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA Kx=DH Au=RSA Enc=Camellia-CBC(256) Mac=SHA1
DHE-RSA-SEED-SHA Kx=DH Au=RSA Enc=SEED-CBC(128) Mac=SHA1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA1
CAMELLIA128-SHA Kx=RSA Au=RSA Enc=Camellia-CBC(128) Mac=SHA1
CAMELLIA256-SHA Kx=RSA Au=RSA Enc=Camellia-CBC(256) Mac=SHA1
SEED-SHA Kx=RSA Au=RSA Enc=SEED-CBC(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

70657 (1) - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/28, Modification date: 2014/04/04

Hosts

163.117.149.128 (tcp/22)

```
Nessus negotiated the following encryption algorithm with the server :
aes128-cbc

The server supports the following options for kex_algorithms :

diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521

The server supports the following options for
server_host_key_algorithms :

ecdsa-sha2-nistp256
ssh-dss
ssh-rsa

The server supports the following options for
encryption_algorithms_client_to_server :

3des-cbc
```

```
aes128-cbc
aes128-ctr
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

The server supports the following options for
encryption_algorithms_server_to_client                    :

3des-cbc
aes128-cbc
aes128-ctr
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

The server supports the following options for
mac_algorithms_client_to_server                           :

hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
hmac-sha2-256
hmac-sha2-256-96
hmac-sha2-512
hmac-sha2-512-96
umac-64@openssh.com

The server supports the following options for
mac_algorithms_server_to_client                           :

hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-ripemd160@openssh.com
hmac-sha1
```

```
hmac-sha1-96
hmac-sha2-256
hmac-sha2-256-96
hmac-sha2-512
hmac-sha2-512-96
umac-64@openssh.com

The server supports the following options for
compression_algorithms_client_to_server                    :

none
zlib@openssh.com

The server supports the following options for
compression_algorithms_server_to_client                    :

none
zlib@openssh.com
```